Intruder Detection System: A Literature Review

[1]Aniket Yadav, [2]Nehal Thaker, [3]Disha Makwana, [4]Ninad Waingankar, [5]Prashant Upadhyay

K J Somaiya Institute of Engineering And Information Technology
Mumbai, India
aniket.sy@somaiya.edu, nehal.thaker@somaiya.edu, disha.makwana@somaiya.edu, ninad.w@somaiya.edu, pupadhay@somaiya.edu

***Abstract*—This paper presents a comprehensive description, from a security and accessibility perspective, of various security automation systems and technologies. For everyone who owns or rents a home, home security should be a top concern. Every individual needs a safe and secure residential space. Most of the market's security systems; however, are either costly or unsafe. Many times there are a number of loopholes present in the security systems and security devices which can be breached easily. The various security automation technologies considered in this review paper include Fiber sensor, Accelerometer, Global Mobile Communication System, Mobile Home Automation Systems, Internet Home Automation Systems. There is a decrease in the price of sensors as we see progress in the technology market, which makes vibration signature identification systems a cheap and effective alternative to the expensive security systems on the market.**

***Index Terms*—IoT, security automation systems, accelerometer, vibration.**

I. Introduction

When you look at your family and house, the first thing you want is their protection. And then the concept of an integrated system of home protection comes into the frame. Since the late 1970's, the idea of home automation and its safety has been around. But our perceptions from home have changed a great deal over the course of time with the advancement of technology and so have the concept of home automation and its security systems. If we look at various home automation systems over the time; they have always tried to provide home residents with reliable, easy, and secure ways of accessing their homes.

IoT is emerging today with a plethora of apps in different sectors, including the security and surveillance industry. The Internet of Things (IoT) refers to a network of linked physical objects that can interact and share data with each other. Modern technical advancements have made it possible to build systems with a combination of hardware and software technology that can operate remotely without any human being being involved or monitored. To build a cost-effective and efficient security automation framework, we can make use of IoT technologies. The systems available are either costly or proprietary so that a user can not afford them or they are forced to be loyal to a particular provider that inhibits the number of choices available to them and prevents them from investing in the security infrastructure required. Intruder detection systems based on IoT can have the security ability integrated with communication features to
alert the intruder's owner even before the intrusion and avoid property damage. We will review the various methodologies and technologies that are used to solve the problem of intruders in the following paper.

II. Literature Survey

A. Intelligent acoustic and vibration recognition/alert systems for security breaching detection, close proximity danger identification, and perimeter protection

Growing focus on the perimeter security of national properties, both at home and abroad, has facilitated the development of technologies capable of detecting possible threats, such as people or vehicles approaching them. One area of interest is the integration of many different sensors, each with its own distinct modalities and detection ranges, to create a flexible and robust device. They propose a device based on three security sensors that have been demonstrated to provide security threat detection and classification. These sensors namely are acoustic, seismic, and vibration sensors. For the detection and reporting of sequential approaching incidents, such as an approaching vehicle with passengers wishing to breach a fenced facility, the 'Smart Fence' device based on these sensors will be particularly suitable. For instance, long-distance vehicles may have a lower level of threat than intruders entering a safe perimeter, which in turn may have a lower level of threat than intruders attempting to climb a fence around the perimeter. The acoustic signatures of interest produced by human and running vehicle approaches are complicated. To detect approaching vehicles and to classify the type of vehicles, they suggest using a

neurobiology motivated algorithm. Nonlinear Hebbian learning (NHL), a simple and appealing neural learning mechanism found in the human brain is used for unsupervised learning with the exact acoustic signature being unknown. The system established can differentiate between three vehicle types, namely light track, heavy track and motorcycle. The purpose of a seismic based human danger detector is to distinguish approaching humans and to differentiate between the series of events caused by the animal and the history of passenger vehicles and a single vibration occurrence, such as the collapse of a tree limb. A geophone-based seismometer was used, which is an inexpensive sensor that offers both simple and immediate deployment and long-range detection capability. In order to model statistical properties of the temporal gait and frequency features extracted from the seismic signals, Gaussian mixture models were developed. To distinguish between human footsteps, cars, backgrounds, the device was set up. A 3-axis accelerometer has been used for fence breach detection and classification purposes. If the breach is due to the rattling caused by strong wind or a person climbing on the fence, the built algorithm based on a non-homogeneous Markov model is able to recognize the form of breaches. On different fences, the proposed algorithm and device have been tested and have shown robust recognition for distinguishing between climb, kick, rattle and context.

B. e-KTP as the basis of home security system using arduino UNO

During the construction of the intruder detection system, there were several systems we encountered. The Arduino UnoR3, ESP8266 NodeMcu WiFi module, alarm, Red Light Emitting Diode (LED) and PIR Sensor are used in the' Arduino-based Wireless Motion Detecting System'[1]. To build this device framework, Android Studio 3.1 software was used. The programming language used in the device application was Java. The transmission of data to the consumer is parallel with the used alarm device. If the alarm device senses movements, applications which have been imported to users' smartphones may cause an alarm. A server-based approach is used by the system so that the user is bound to the Internet. The Arduino Uno microcontroller is used as a doormat in a door-based digital home protection system in the 'e-KTP as the basis of the home security system using Arduino Uno'[2] Radio Frequency Identification (RFID) system from e-KTP. The data stored on the e-KTP card will be transmitted to the RFID Reader when the power is switched on and an e KTP card is present. If the check is ineffective, a "threshold" warning will be generated, the red light will be switched on, and an alarm will be generated to identify that the robbery has occurred in the building. To build a database for e-KTP on the internet, a XAMPP server was used.

C. Low Power Accelerometer Based Intrusion and Tamper Detector

Intrusion detection systems (IDSs) use a wide range of sensors to identify unauthorized attempts to enter secure arenas and to provide security response teams with warning signals as well. Passive infrared (PIR) sensors, proximity sensors, microwave sensors, video detectors and magnetic switches are the major sensor technologies for interior safety. Another modality of sensing is used in this paper: because most intrusions cause vibrations, it can be sensed to create a detector. For tamper detection, the proposed sensor may also be used when the unauthorized movement of protected objects can be detected using the vibration induced by the attack. In terms of deployment, wireless sensors provide greater comfort than their wired counterparts, because no sensor wiring or cabling is needed. Power can easily be given for wired detectors, but this is not the case for wireless sensors, and power efficiency is a key design factor. Duty-cycling will minimize the power consumption of a sensor: the sensor is worked for a short duration and turned off for another period of time in order to save electricity. The longer the sleep time, the more energy can be spared, vs. the awake time. Sensing capabilities must of course be maintained, so sensors must spend ample time awake. A novel sensor using inexpensive MEMS accelerometers and a simple mechanical system is proposed in this paper, expanding the sensor's capabilities to provide low-energy operation. The time between two sensor awakenings when duty-cycling is used must be trivially shorter than the duration of the event to be detected. This reality restricts the feasible duty cycle, provided an event form. Vibrations are used in the proposed solution to detect unwanted attempts, so the duration of the vibration induced by various acts must be taken into account. However, we use a hardware extension of the sensor in our proposed solution, which prolongs the impact of the event in time; thereby allowing lower duty cycles and lower energy consumption. This paper proposes a novel energy-efficient MEMS accelerometer-based sensor that can be used as an intrusion or temper detector. The sensor is based on a low-cost BMA180 accelerometer with a simple mechanical extension that allows for the elongation of time events and thus lower duty cycle activity. The proposed sensor performed extremely well in performance tests (100 percent hit rate) with service cycles as low as 5-10 percent. The sensor's low power consumption allows it to be used in wireless

(e.g. ZigBee) networks.

D. IoT based Intruder Detection System Using GSM

The Internet of Things (IoT) is a network of interconnected objects that can interact and share data. The combination of software and hardware developments has allowed the development of systems that can run remotely without the need for human interaction. Theft and burglaries are rising at an exponential pace all over the world. Various news outlets have written on such events, which occur while the house's occupants are not present. Intruders will often break in even though the occupants are present. This is a dilemma that everybody has to contend with. The available systems are either too costly or too proprietary for a consumer to afford, or they are forced to be loyal to a single vendor, restricting their options and preventing them from investing in the necessary security infrastructure. The paper proposes a low-cost, scalable and low-maintenance intruder detection system to solve these issues. The proposed device would not act like any of the currently available protective devices, which do not warn the consumer when an intrusion occurs. This device notifies the user when a disruption happens, so it does not produce any false alarms. The hardware module and a mobile application make up the framework. When the hardware module senses any movement, it sends a warning to the app's users. As soon as the device is activated, it will send a message to the application, alerting it. The aim of this project is to build an intruder detection application using an AVR microcontroller device, conduct User Acceptance Testing and implement an external beta tester. Since our device is modular, the user can add as many hardware modules as they want. The software can be used by either home or shop owners to receive alerts in the event of any unauthorised intrusions. In order to detect an intrusion, the sensors MC-38 (magnetic switch) and SW-420 (vibration sensor) are used to implement the device. The code created in the Arduino IDE was uploaded to the atmega 8A using an FTDI programmer. When the sensors are activated, a sim 800L warning is sent to the application. Android Studio was used to develop the software. The hardware device detects the intrusion and notifies the programme successfully. The device's versatility allows it to be incorporated into existing security infrastructure. The device's simplicity makes it perfect for scaling up to meet the needs of the consumer. The device's hardware is built in a modular manner, enabling it to be easily enhanced by connecting it to a wireless sensor network. The system can be upgraded by adding an internet module in addition to the GSM module. This would allow the computer to switch between the two communication interfaces easily when one is inaccessible, improving the system's overall performance.

E. Fuzzy logic based method to estimate the risk of alarm system false detection

An alarm system's primary purpose is to identify, prevent and document/inform about any intrusion into a secure area or facility. False alarms complicate the identification problem when the facilities or areas are situated in areas of varying environmental factors. The process of adapting alarm system detectors to a particular location could be accomplished, but it would take a long time and increase the system's cost. Knowing the characteristics, in particular the possibility of intruder detection; false alarm rate will have an alarm system before its implementation is a quicker and less costly way. As a consequence, the proposed method for obtaining such characteristic values is valid. There are a number of factors that impact proper detection. Intruder features and climatic sounds can be distinguished. The volume and pattern of emitted energy, the size of the object, the distance to the object, the speed of the moving object, the direction of the movement, and the reflection/absorption characteristics of the energy waves by the intruder and the environment are all intruder variables that usually influence the likelihood of detection (e.g. open, shrubbery, or wooded area). Powerful wind, rain, snow or fog according to climatic noises; motion of small and large animals, birds, according to mechanical noises. Lightning, air, and underground high-voltage lines both produce electromagnetic noise. The values of the enumerated factors' characteristics, on the other hand, were not presented in, i.e. there are no objective descriptions of any physical quantity that defines strong wind, precipitation level, etc. Interval numbers can be used when the lower and upper limits of the characteristic values are known. However, if any experimental or expert data is available, one of the simple (triangular, S-shaped, Z-shaped) fuzzy membership functions may be used to define the characteristics: lower, upper limits, and - most likely - the value. In the case of small sample sizes, using complex membership functions is impractical. The method for estimating the probability of false alarm detection in an alarm system was developed. It takes into account the noise's strength as well as the detectors' susceptibility to it. By taking climatic conditions into account, it is possible to reduce the volume of Pareto-optimal sets of alarm systems.

F. Identification of Damaging Activities for Perimeter Security

Both the nation and individuals have recently put a greater focus on perimeter security for the house, national border line, airport, military base, transportation hub or oil and gas pipelines among other items. A perimeter protection system should have the following capabilities: 1) it should be able to relay signals over long distances and track in real time during the day in all weather conditions; 2) it should be intelligently sensitive to the environment to easily discern dangerous activities from routine activities; and 3) it should be able to adjust to new environmental changes. Intruders are detected using ultrasonic, microwave, infrared or photoelectric sensors in conventional perimeter protection systems. However, since these sensors need power, their detection range is limited. Fiber sensors have been successfully used in perimeter security since the introduction of fibers sensing technology. Fiber sensors have many advantages over other sensors, including a simple structure, low cost, long-distance communication capability, accurate positioning and energy savings. It can also sense the atmosphere and relay signals. A perimeter protection system based on fiber has been developed. Unfortunately, due to its low intelligence, the machine is unable to decide what form of harmful activity has occurred. Wang offers a long distance safety monitoring device for buried oil pipelines based on fibre sensors. He also explores vibration signals. However, only frequency data is taken into account, and only three forms of harmful behaviors are listed. This paper builds on our previous work [7, 8] by concentrating on making the perimeter security system more intelligent, i.e., allowing it to detect more dangerous activities. We obtain a feature vector of each vibration signal fragment using both statistical analysis by Gram-Charlier series and time-frequency analysis by wavelet packet decomposition using vibration signals obtained by a fiber sensor as data source. We suggest a method to find the second best wavelet packet bases since the best wavelet packet bases do not exist for all signals. For de-correlation, independent component analysis (ICA) is used. In the classification process, a kernel space hierarchy clustering-based SVM tree algorithm is also presented. The effectiveness of the proposed feature extraction classification method for identifying damaging activities using vibration signals obtained from fibre sensors has been demonstrated. In the future, we will undertake comprehensive research into new forms of dangerous behaviours. Furthermore, the vibration signals of various types of activities have several distinct time domain evolution characteristics, such as the trend and length of the vibration signal. This form of character has not been completely used, which is something that should be considered. In addition, we can use online incremental learning to train for potential applications in the real world.

G. Home security system using internet of things

The Internet of Things (IoT) is a network of interconnected physical objects that can interact and exchange data without needing human interference. Since IoT permits the US to gather info from every kind of medium, like humans, animals, vehicles, and room appliances, it's been formally outlined as a "Infrastructure of data Society." By embedding electronic hardware like sensors, software, and networking gear into any entity within the physical world which will be a science address to permit information transmission over a network, it will become a vicinity of the IoT framework. IoT is distinct from the Internet in that it goes beyond Internet access by allowing ordinary artifacts with embedded circuits to interact and communicate with one another using existing Internet infrastructure. The word "internet of things" and its creation can be traced back to a speech given by Peter T Lewis at the Federal Communications Commission in 1985. (FCC).

Since then the Internet of Things has expanded exponentially, with more than 12 billion connected devices now in operation with analysts expecting that number to hit 50 billion by the end of 2020. The Internet of Things technology has aided decision-making by offering real-time data collection and analysis using precise sensors and seamless communication. Both producers and customers have benefited from the Internet of Things. Manufacturers have gained insight into how their goods are used and work in the real world, enabling them to maximise sales by offering value added services that prolong the life cycle of their products or services. Consumers on the other hand can attach and monitor several devices for a more personalised and enhanced user experience. When it comes to home automation, security is a significant aspect. Home security is one of the most important aspects of home automation; if not the most important. Home security has advanced significantly in recent decades and will continue to do so in the coming years. Home security systems used to mean getting an alarm that would go off if anyone broke in, but a smart safe home can do so much more. As a result, the main purpose of our work is to build a device that can send a warning to the owner and others in the event of an intruder break-in. The alarm would also be able to be

stopped or started remotely using the owner's mobile. Users will be able to protect their homes by installing the device on their doors or windows and tracking activity through their smartphones.

Since the last few years, the number of devices connected to the Internet has risen at an exponential pace. All of these internet-connected devices are part of the IoT infrastructure, which enables them to send and receive data from one another. This is why it is advantageous to design the proposed security framework using an existing infrastructure. When a user is not present in the home to take action an alarm that sounds like the buzzer is useless. When the owner is gone, keep in touch with one another. They want to know that their home is safe from intruders and criminals when they are abroad, so they set up an IoT network with embedded electronics, sensors and apps at their home. As a result, the proposed system keeps the owner up to date on the security status of their home in real time. The built system warns the user when there has been a break-in, enabling the user to take appropriate action.

H. Securing IoT Devices and Securely Connecting the Dots Using REST API and Middleware

The Internet of Things links computing devices embedded in everyday objects to the Internet so that they can send and receive data. There are two benefits: we can enable our machines to gather information about our environment without relying on humans and we can also minimise extravagance, failure, and expense by processing the information gathered. The Internet of Things allows physical and digital worlds to communicate with one another. Sensors and actuators enable the digital and physical worlds to connect. These sensors gather data that needs to be stored and analysed. Data processing may take place at the network's edge on a remote server or in the cloud. An IoT object's storage and processing capacities are limited by the resources available; which are limited by size, energy, power and computational capacity. As a result, these systems depend on IoT middleware to provide the necessary functionality.

I. Automatic Service Request System for Security in Smart Home Using IoT

Because of the benefits of automation, new homes will become smarter and more automated. Users can monitor various electric and electronic appliances using an automation system in a smart home. One of the most pressing issues is the safety and protection of one's home. People's safety and protection, as well as their property are now possible thanks to technological advancements. One of the driving factors behind the growth of the smart home is the need to reduce the risk of theft, robbery and accidents. People want to track the state of their home remotely due to their hectic lifestyles. The consumer can track the status of the home in most current smart homes, but there is no guarantee of safety or protection. The Internet of Things (IoT) is critical for integrating security features in smart homes.

A microcontroller is made up of various functional blocks such as a general-purpose processor, memory, GPIO and communication. When compared to troubleshooting, implementing a system is easy. So if an anomaly is discovered, the user must request service to resolve the issue. When an abnormality occurs, the proposed framework will notify both the customer and the concerned service providers according to this article. The intrusion device for example, would alert both the user and the security individual.

This project implements an automated service request system using an Advanced RISC machine (ARM) controller and the Internet of Things (IoT). These Raspberry Pi-based systems are easy to incorporate in practise and the majority of them can be effectively used in real-world applications. Since the Arm Controller is a 64-bit controller it offers more benefits than traditional 8-bit or 16-bit microcontrollers. Also it has a high code density and good interrupt response, the Arm architecture is based on Reduced Instruction Set Computer (RISC) rather than traditional complex instruction set computer (CISC). This allows it to be used for real-time applications. Since this is based on a pipelining mechanism, the controller's output is excellent. In a pipelining mechanism, instructions are processed in parallel using three separate cycles of fetch, decode and execute, i.e., when one instruction is executed, the next instruction is decoded and the next instruction is fetched from memory to the processor.

J. A Smart IoT Security System for Smart-Home Using Motion Detection and Facial Recognition

A smart home is made up of a computer, a smartphone and other smart sensors or actuators with an Internet of Things link. The Internet of Things (IoT) consists of interconnected computing devices that transmit data over a network without requiring user interaction. This provides a forum for a security system by encouraging the user to feel secure at home and leave the house trusting that they will be notified if anyone approaches the house. The definition of protection and safety is one area where technology can help us. The fact that the majority of our population now carries technology on their person, as opposed to earlier years of smartphones, makes the idea of smartphones acting as a security warning system more appealing. Two factors are needed for proactive crime prevention:

time and facts.

Individuals can now track house/office/store security conditions on a continuous basis; thanks to the recent increase in availability and usage of smart IoT devices and the ubiquity of smartphones. This project's major impact for society is to establish a viable and easily available approach to the community by gathering data and identifying risky behaviors in the smart-home environment. In this research, we developed a system (smart IoT system) that allows the user to detect unauthenticated access in the smart-home.

K. Security and Privacy of Smart Home Systems Based on the Internet of Things and Stereo Matching Algorithms

People's demand for a safe, comfortable and intelligent living environment is becoming more urgent as the economy, living conditions, and the environment deteriorate. A smart home is becoming increasingly popular. Future life can be more intelligent, consume less resources and make better use of renewable energy. The safety factor of smart homes has improved as technology has progressed. Automatic control technology, awareness technology, mobile communication technology, audio and video processing technology and other technologies are all integrated into smart homes. Smart home technology has steadily made its way into the average home.

Despite the fact that some technologies are fairly mature, there is still a lot of room for innovation in this sector. Smart home systems focused on the Internet of Things (IoT) have inevitably become a research hotspot in recent years. As a consequence, this article delves into the viability of smart home

device design from both a hardware and software perspective. Using the stereo matching algorithm, the device information is analysed and monitored accurately by constructing the application of an IoT module. The system's overall structure has been strengthened, ensuring the security and intelligence of users' homes while also encouraging the production of smart homes.

L. Theft Detection System using PIR Sensor

The world has changed drastically as a result of technological advances. Because in the rapid advancement of technology, the next century would be more comfortable. The Internet of Things (IoT) is a new technology that is gaining traction in the real world. This technology has a promising future in making the whole system smart. The development was the smart surveillance system. There were lots of inventions developed in the field of IoT and the most recognized one was the smart surveillance system development. There were lots of advancements in wireless technologies such as domain, cloud and many other technologies which were included in the system to show something new.

Many devices; such as electronic, electrical and IT-related works, would be included in the Internet of Things. A smart surveillance system consists of several devices that must be carefully controlled and managed so that the system does not malfunction due to inappropriate software handling. The lack of connectivity is a problem that people face after a few days. The smart surveillance system is one of several IoT applications that is crucial to the realisation of smart cities. The Indian government has proposed the development of numerous smart cities across the country, which will result in a significant increase in demand for smart home automation solutions in the near future. The term ”smart” in surveillance refers to context-awareness, which can be achieved by the use of IT and IoT.

M. Ambient Intelligence and IoT Based Decision Support System for Intruder Detection

Ambient intelligence (AmI) is a ubiquitous computing environment that provides autonomous services in response to user needs and accepts feedback through gestures, speech and other non-intrusive methods. Embeddedness, openness, context awareness and machine learning are all core components of ambient intelligence. Computers are not self-contained systems; but rather a man-made platform with built-in intelligence and computational capabilities, resulting in embedded computing. In the sense of AmI, transparency refers to people automatically engaging with their environment rather than picking up a tablet and typing in a query. Context knowledge refers to the software and hardware working together to collect and interpret data in order to direct responses. By learning from experience and expanding capacity autonomously, machine learning leads to potential effectiveness.IoT makes data accessible all over the world; which, like ML is a rapidly growing trend.

Robbery, commercial and economic fraud and trafficking in illicit goods or imports and services are all on the rise in the twenty-first century. While there are many ways to avoid this in the corporate world, only a few services have been applied to ordinary people's lives. Many unusual events occur in daily lives and if they are not recognised in a timely manner, they may result in dangerous consequences. An individual getting a heart attack, a robbery at home, or a gas leak in the kitchen are all examples of anomalies. Ambient intelligence considers these aspects and can provide a family with a worry-free life by having home protection. The

majority of home security systems focus solely on protecting entry points such as doors, windows and valuables. These systems will be made up of networks of interconnected electronic devices. For ambient assisted living, smart homes now use environment aware technologies. The emphasis of this paper is on providing indoor protection for a healthy and stable living environment.

The remainder of the paper is organised as follows: division 2 outlines related field work, division 3 offers a framework summary, division 4 illustrates methodology, and division 5 displays the results obtained. Division 6 includes a review of the proposed work as well as proposals for future changes.

N. IoT Based Mobile Smart Home Surveillance Application

Human beings have been working hard to improve their living conditions. The development activities have been driven by the demands of human beings in relation to the time period in which they live. The industrial revolution began with the invention of the coal-burning steam engine and progressed with the use of electric power in mass manufacturing, culminating in the fourth industrial revolution with the advent of cyber physical structures and the Internet of Things (IoT). With the advances provided by the digital world, IoT technology is rapidly changing our life standards. Kevin Ashton invented the word ”internet of things" in 1999, and the International Telecommunication Union formally adopted it in 2005. Smart devices with identity, networking and processing capabilities can connect with one another using IoT, networking and communication technologies to accomplish different goals regardless of their geographic location. The Internet of Things is made up of four components: entity, data, processing and humans. Each component presents its own set of difficulties and opportunities.

The Internet of Things (IoT) is very common these days because it allows people to view, handle and monitor IoT objects from afar for social good. As a result, the Internet of Things (IoT) technology will allow developers to help the public by creating profitable applications in a number of fields, including business, education, agriculture, manufacturing, healthcare and emergency services, government, transportation, smart home, smart factory, smart city, industry, electricity, tourism and many others. Furthermore, the IoT technology plays an important role particularly in ensuring the data exchange between objects. Especially in this data era, accessing, collecting, harnessing and analyzing data collected from various IoT objects is very important to make the right actions within the right time.

Furthermore, smart homes provide residents with convenience, comfort, protection and energy efficiency. To remotely control smart home automation systems, most researchers are now using web services such as Soap and restful services.

Residents can monitor smart home systems from afar using a smartphone application for a variety of purposes. For example, in smart homes, using temperature sensors to monitor and adjust the mode of the heating system (activate/deactivate), using motion sensors to switch the lights on and off when motion is detected and even turning on the lights when you return home after a long day can be extremely inconvenient and exhausting. Smart home systems make our lives simpler in a number of ways. As a result, we created a mobile application for our smart home system that allows us to monitor lighting, heating, humidity, and gas units. When motion is detected in a room, our mobile application connects to the smart home system and controls the lamp to be switched on/off manually. In addition, the mobile application will regularly collect and store gas, temperature, and humidity data in order to gain insight and knowledge. When an irregular or emergency condition is identified in the smart home system, our mobile application will send email alerts to users.

O. IoT based Smart Home Surveillance and Automation Since monitoring and surveillance 24 hours a day, seven days a week is difficult to manage manually, protection at living species has become important for current lifestyles. One of the best options is to use the latest technologies in IoT applications. We can get information about security risks, damage warnings and danger alerts, as well as additional controls over home appliances for comfort, automation and home surveillance by using IoT.

For automation and surveillance, the Raspberry Pi board monitors and guides the sensing transducers and visionary sensors. Smart home refers to a home with sophisticated automatic systems that are pre-programmed for tasks such as controlling door and windows, LPG leakage detection, and fire detection, among others. Home automation is also on the increase, as smartphones have become more user-friendly and low-cost. As a result of the adoption of various advanced wireless communication technologies and methodologies (GSM, WIFI, Bluetooth). The Internet of Things (IoT) is a technology that can alter a user’s lifestyle. That is to say, that the internet has changed the way we function and connect with those on the internet. IoT helps you to interact from anywhere with electrical and electronic devices that are used in your home. The addition of knowledge; such as Raspberry Pi allows us to run and monitor the home appliance at our leisure

Sr No.	Paper title	Technologies used	Strengths	Weakness
1	”e-KTP as the basis of home security system using arduinoUNO”	RFID	i) Only unique ID number can give access to open door ii) Web based logging system	i) Metals and liquids can impact signal
2	”Intelligent acoustic and vibration recognition/alert systems for security breaching detection, close proximity danger identification, and perimeter protection”	Acoustic and Vibration Recognition	i) seismic analyzer which discriminates between human footsteps and other seismic events ii) False signal detection	i) Practically not accurate
3	”Low power accelerometer based intrusion and tamper detector”	Vibration analysis using Accelerometer	i) Cost effective ii) Effective vibration sensing iii) Low power consumption	i) Implementation is difficult
4	“IoT based Intruder Detection System Using GSM”	GSM	i) Alert warning to owner ii) Simple and easy implementation	i) Not efficient ii) Not much reliable
5	”Fuzzy logic based method to estimate the risk of alarm system false detection,”	Fuzzy logic	i) Accurate sensing of data ii) Environmental signal and noise can be distinguished	i) Special sensors required ii) Expensive
6	”Identification of Damaging Activities for Perimeter Security”	Support Vector Machine (ML)	i) Feature extraction ii) Accurate data analysis	i) Improvement for incremental learning ability
7	“Home security system using internet of things”	Arduino UNO	i) Open source ii) Easy implementation	i) Not reliable ii) Not secure
8	Securing IoT Devices and SecurelyConnecting the Dots Using REST API and Middleware	Rest API	i) End to end encryption ii) Secure IOT devices	i) Resource constraints
9	Automatic Service Request System for Security in Smart Home Using IoT	Raspberry PI	i) Multipurpose use such as security, fire safety etc	i) More complex ii) Expensive
10	A Smart IoT Security System for Smart-Home Using Motion Detection and Facial Recognition	Motion detection Facial recognition	i) High degree of classification ii) Accurate security sensing	i) Low processing power ii) Huge database required
11	Security and Privacy of Smart Home Systems Based on the Internet of Things and Stereo Matching Algorithms	Stereo matching algorithms	i) Highly secured network ii) Easy home automation and security	i) Bulky ii) Expensive
12	Theft Detection System using PIR Sensor	PIR sensor	i) Real time video sensing ii) Direct surveillance	i) Precautions measures by owner
13	Ambient Intelligence and IoT Based Decision Support System for Intruder Detection	Face detection	Accurate human face sensing	Not useful for non-human security breaches
14	IoT Based Mobile Smart Home Surveillance Application	NodeMCU Wifi module	Smart Home monitor	i) Lack of database ii) Less sensors iii) Not reliable for security options
15	IoT based Smart Home Surveillance and Automation	GSM, Raspberry PI	Home Security Surveillance System	i) Easy to attack ii) Data leakage

III. Conclusion

Our work mainly concentrates on the application aspects of the numerous intruder system and also points out the various involvement of technologies used to make the intruder detection system practical for real-life application. We summarized the various systems that utilizes low-cost components while having potential for industry standard usage. We encourage researchers to think about home automation as one of the most critical aspects of home protection and to develop advanced sensing technologies to detect and secure homes from professional intruders. When it comes to the proper implementation and production of automated home protection systems, the most important factor is security. Such a device will give everyone in the house a sense of security and will also put their minds at ease. Sensing the correct data is essential for correct security breach detection. False detection is very important which gets ignored in many theft detection systems. Today data science can be used to trace a lot of information about the security environment. IOT plays a major role in theft detection and exchanging the data over the cloud. As we progressed IOT architecture and sensors became more budget friendly. We can use different types of sensors such as vibration sensing accelerometer, reed switches, PIR sensors. Data analysis on these sensor's data can achieve highly useful data even using simple sensing. Hence, we recommend IOT and Data analysis on sensor's data can bring the new heights in theft detection systems.

References

[1] M. Andriansyah, M. Subali, I. Purwanto, S. A. Irianto and R. A.Pramono, "e-KTP as the basis of home security system using arduino UNO," 2017 4th International Conference on Computer Application And Information Processing Technology (CAIPT), Kuta Bali, 2017, pp.1-5

[2] A. A. Dibazar, A. Yousefi, H. O. Park, B. Lu, S. George and T. W. Berger, "Intelligent acoustic and vibration recognition/alert systems for security breaching detection, close proximity danger identification, and perimeter protection," 2010 IEEE International Conference on Technologies for Homeland Security (HST), Waltham, MA, 2010, pp. 351-356, doi: 10.1109/THS.2010.5654931

[3] G. Vakulya and G. Simon, "Low power accelerometer based intrusion and tamper detector," 2014 IEEE 11th International Multi-Conference on Systems, Signals Devices (SSD14), Barcelona, Spain, 2014, pp. 1-6, doi: 10.1109/SSD.2014.6808878

[4] Iyer Saikumar, Gaonkar Pranjal, Wadekar Shweta, Kohmaria Nayan and Upadhyay Prashant, IoT based Intruder Detection System Using GSM (April 8, 2020). Proceedings of the 3rd International Conference on Advances in Science Technology (ICAST) 2020, Available at SSRN: https://ssrn.com/abstract=3572326 or http://dx.doi.org/10.2139/ssrn.3572326

[5] Zhengbing Hu, V. Nimko and P. Bykovyy, "Fuzzy logic based method to estimate the risk of alarm system false detection," Proceedings of International Conference on Modern Problem of Radio Engineering, Telecommunications and Computer Science, Lviv, UKraine, 2012, pp. 452-453

[6] H. Yan, G. Shi, Q. Wang and S. Hao, "Identification of Damaging Activities for Perimeter Security," 2009 International Conference on Signal Processing Systems, Singapore, 2009, pp. 162-166, doi: 10.1109/ICSPS.2009.17

[7] A Anitha, "Home security system using internet of things" 2017 IOP Conf. Ser.: Mater. Sci. Eng 263 042026

[8] Hittu Garg,Mayank Dave, "Securing IoT Devices and Securely Connecting the Dots Using REST API and Middleware,"978-1-7281-1253-4/19/ 31.00, 2019 IEEE

[9] Pranav Kumar Madupu, Karthikeyan B, "Automatic Service Request System for Security in Smart Home Using IoT," 978-1-5386-0965-1/18/ 31.00, 2018 IEEE

[10] AKM Jahangir Alam Majumder and Joshua Aaron Izaguirre, "A Smart IoT Security System for Smart-Home Using Motion Detection and Facial Recognition," 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)

[11] Aimin Yang , Chunying Zhang , Yongjie Chen, Yunxi Zhuansun, and Huixiang Liu ,"Security and Privacy of Smart Home Systems Based on the Internet of Things and Stereo Matching Algorithms,"IEEE INTERNET OF THINGS JOURNAL, VOL. 7, NO. 4, APRIL 2020

[12] Prithvi Nath Saranu, Abirami G, Sivakumar S, RameshKumar M, Arul U, Seetha J "Theft Detection System using PIR Sensor," 978-1-5386- 3695-431.00, 2018 IEEE

[13] Lashmi.K, Anju.S.Pillai, "Ambient Intelligence and IoT Based Decision Support System for Intruder Detection,"978-1-5386-8158-9/19/31.00, 2019 IEEE

[14] Haki Mehmet ERZ, Ahmet Arif AYDIN, "IoT Based Mobile Smart Home Surveillance Application," 978-1-7281-9090-7/20/31.00 ,2020 IEEE

[15] Sandeep Kumar, V. Taj Kiran, Sekuri Swetha, Prashant Johri, "IoT based Smart Home Surveillance and Automation," 2018 International Conference on Computing, Power and Communication Technologies (GUCON) Galgotias University, Greater Noida, UP, India. Sep 28-29, 2018