DisSERTATION PROPOSAL

ELISHA DHUNGANA

21061524

An IOT based Anti-theft security system

Table of Contents

[1 Project Title: 2](#_Toc111148030)

[2 Aims: 2](#_Toc111148031)

[3 Objectives: 2](#_Toc111148032)

[4 Scope: 2](#_Toc111148033)

[5 Introduction to the project: 3](#_Toc111148034)

[6 Problem Statement 3](#_Toc111148035)

[7 Background, Motivation and Relevance – literature review 4](#_Toc111148036)

[7.1 Background Reading 4](#_Toc111148037)

[7.1.1 Understanding of IOT: 4](#_Toc111148038)

[7.1.2 IOT frameworks- Arduino: 6](#_Toc111148039)

[7.1.3 Technical Requirements of the System: 6](#_Toc111148040)

[7.2 Motivation 7](#_Toc111148041)

[7.3 Literature Review 7](#_Toc111148042)

[8 Research Methodology 8](#_Toc111148043)

[9 Project Planning 9](#_Toc111148044)

[10 Conclusion 9](#_Toc111148045)

[11 References 10](#_Toc111148046)

# Project Title:

An IOT based Anti-theft security system

# Aims:

The aim of this proposed system is to investigate on Anti-theft IOT based Security system and to develop a user solution application that supervises and tracks the item in real-time if a person attempts to enter a restricted area or changes the object`s position.

# Objectives:

* To study and investigate about the IOT based home security system using Arduino.
* To compare and evaluate between Arduino and Raspberry pi framework of IOT which are applicable for the home security.
* To research about appropriate sensors used in IOT for the home/ office security.
* To analyze the integration of mobile apps with IOT sensors within the IOS and Android platform.
* To design a security system model that can ring an alarm whenever someone steps into or touches a prohibited area.
* To develop a mobile application that can send the user an immediate text message alert in the event of an external occurrence, such a theft.

# Scope:

The goal of this project is to create a monitoring` system that can immediately respond to motion detection by sending an alarm to the administrator device via a mobile application. The scope of this initiative is to prevent theft in private residences, jewelry stores, offices, retail establishments, and even in public places that are restricted.

Arduino Uno, Wifi-Shield 2 for Arduino, a relay, a force sensor, a resistor, jumper wires, a warning light, and an electronic horn are all necessary components for the system. The user can check on the machine from a distance. However, neither the motion sensing device nor the Arduino UNO will be attempted to be designed for this project. Therefore, it will leverage these systems along with an appropriate application script to implement the needed real-time monitoring system.

# Introduction to the project:

The concept of home automation and its safety has been introduced around since late 1970s. Previously home security systems meant having an alarm that would go off when somebody would break in, but a smart secure home can do much more than that. With the advancement of technology, our expectation from home has changed a lot and so have the idea of home automation and its security systems has evolved. If we look at different home automation systems over time, they have always tried to provide efficient, convenient, and safe ways for home inhabitants to access their homes.

Home security made a drastic change in the past few decades and continue to advance much more in the coming years. Despite evolving technology and changing consumer expectations, a home security system still serves the same purpose. Proper timely precautions can save you and your property and expensive items with all such consequences. Therefore, installing a smart Anti-theft security system can turn the house/office into a safe place that can be the answer to all these robbery and theft issues, provided that a security system is hassle-free and user-friendly.

By using the concept of IOT, the proposed system will be developed on Arduino Platform by using the technique with Arduino UNO with IOT and moreover, it is done by integrating sensors which is integrated to a mobile application(Johri, n.d.). The project is designed to help an individual secure his/her object/item from stolen.

It is also essential that the system must be compact and easily maintained. Therefore, the proposed system consists of mobile app that controls the whole system. The system goes live using the command received from the applications and all the sensors are activated.

# Problem Statement

Incidents like thefts, snatching and robbery are very common these days. Some people simply do not have time to take care and protect their valuable items from theft. Others need a security solution for the valuable object like money, gadgets, and jewelry when they are not at home or office. The most effective deterrents for home burglaries and theft are only limited to CCTV monitoring in the past decades. Considering those incidents, home security had made a drastic change in the past few decades and continue to advance much more in the coming years (Edwards, 2022).

These problems demand a solution which can track the item in real-time if the thief enters the restricted area or any items he picks. Therefore, the project is proposed to design an integrated home security system that would help people secure their houses from such challenges.

# Background, Motivation and Relevance – literature review

## Background Reading

The main objective of this paper is to implement an Anti-theft IOT based system for item tracking which must be easily handled by the owner and protects the valuable assets by alerting the owner immediately in cases of chances of theft. Additionally, the system must be portable and simple to maintain. As a result, the suggested system needs a lot of previous knowledge on IOT-based home security and its framework.

### Understanding of IOT:

In 1999, Kevin Ashton, executive director of MIT's AutoIDCentre, coined the term "Internet of Things.". During the same year, they discovered a global RFID-based item detection system (Ashton,1999). Internet of Things (IOT) is basically, the network of ‘things’ by which physical things can exchange data with the help of sensors, electronics, software, and connectivity (Saha, 2021).

Technology continues to advance, and smart devices continue to become more prevalent, the t demand for ubiquitous context-aware platforms that support interconnected, diverse, and distributed networks of devices which is referred as Internet of Things (IOT). (Khodadadi & Buyya, 2017). Simply, IOT is explained as a communication and connection between humans and the technological devices via the internet. Sensors are used extensively in IoT to perform most processes and it is deployed in all the places which converts raw physical data into digital signals and transmits them to the control center(Suresh et al., 2014).

Graphical user interface

Description automatically generated

Figure: IOT HISTORY (Bear, 2019)

IoT devices generate a lot of data, such as logs and analytics, which can be tracked and analyzed to not only track performance but also proactively find and fix security vulnerabilities. Using the appropriate IOT sensors, tools, and best practices (Klein, 2019).

Diagram

Description automatically generated

Figure: The process of IOT system (Sensors in Internet of Things(IoT) - GeeksforGeeks, 2021)

Initially, Sensors collect the data from the environment. Connecting sensors and devices to the cloud can be achieved by using cellular, satellite, WiFi, Bluetooth, low-power wide-area networks (LPWAN), or by connecting directly to the internet using Ethernet. Whenever data is stored in the cloud, it is processed by software. As a next step, the end-user is made aware of the information in some way.

A user could be alerted via email, text, notification, etc. For instance, a text message alarm when the cold storage facility's temperature rises too high (McClelland, 2017).

### IOT frameworks- Arduino:

The greatest platform for learning the fundamentals of embedded system is Arduino. This platform allows a scholar to put into practice all they have studied in class regarding sensors, LEDs, switches, and other topics. As a result of recent advancements in information and communication technologies, a digital transition is currently underway (ICTs). These have a favorable effect on every area of technology and offer connectedness and ubiquity that were unthinkable just a few years ago.

Using the Arduino IoT Cloud application, it is secure and straightforward to create the link between Multiple devices which can be connected to one another to communicate real-time data.

A close-up of a circuit board

Description automatically generated with medium confidence

Figure: Arduino Device

### Technical Requirements of the System:

There are specific hardware and software requirements for the proposed system, which are described below.

#### Hardware Requirements

* Arduino UNO
* Bolt Wi-Fi Module
* Breadboard
* Male/Female Jumper Wires
* Force Sensor
* Buzzer
* Resistor
* LED
* USB-A to B Cable
* USB-A to Mini-USB Cable
* Mobile phone

#### Software Requirements

* Arduino IDE
* IOT bolt Cloud
* Bolt IOT Android Platform
* Android Studio
* Ubuntu Server
* Python 3.8

## Motivation

In most of the home security system that were designed earlier have many limitations and drawbacks, such as being vulnerable to power outages and compromising security. Data backup and real-time observing arrangement is necessary for security monitoring systems to minimalize with the security breakdowns. Therefore,

## Literature Review

K. Hemasaisiva prasad et al.(2016) has proposed structure that assures the creation of an innovative anti-theft ATM system based on IoT technology. A comprehensive and efficient solution for mobile payment security was put forth in this project. It can be placed in the ATM in a secure spot where robbers cannot access it. The solutions currently in operation are simply incredibly expensive and ineffective from either a distance, which is how the suggested approach differentiates from existing ATM intrusion and theft control devices. dependable, economical, and acceptable construction.

Govinda et al. (2014) discussed Design and Implementation of Security for Smart Homes based on GSM Technology, which offers two ways to establish home security utilizing IoT. One method is to use web cameras so that if the camera detects motion, it rings an alarm and emails the owner. Despite being rather expensive due to the cost of the cameras used, this method of detecting incursion is highly effective. The cameras must be of good quality to be able to detect movement. This means that they must have a wide field of view. Additionally, mobile cameras like dome cameras would cost even more than fixed ones if you choose them.

Karri and Daniel (2005) presented an SMS-based system utilizing GSM that would leverage internet services in place of traditional SMS to convey messages or alerts to the homeowner.

Jayashri and Arvind (2013) developed a fingerprint-based identification system to unlock the entrance door. By only permitting users whose fingerprints have been verified by the home's owner, this approach benefits users. This technique can also be used to keep track of who has entered the house using the sensor. The system is combined with a few other capabilities for home security, including ones for gas leaks and fires. Although an excellent technology, fingerprint sensors are expensive and difficult to integrate into an IoT setup since they require improved sensor resolution.

It is always recommended to use fingerprint scanners in two factor authentication systems where an additional layer of security is available in the form of PIN, passcode, voice recognition, etc. Some experts also contend that relying solely on a fingerprint sensor is not wise because it is relatively simple to lift someone's fingerprints and replicate them.

Some researchers put forth the concept of a reliable Internet of Things home security system where the failure of one system component does not result in the failure of the entire system.

The concept of using several devices, some of which may or may not be directly compatible, but which may be configured to function so that they can take the place of an existing system component in the event of a malfunction. Along with this, the model has the capability of using overlap between different devices, which would result in energy conservation and increase the model's efficiency. In the scenario given, a broken camera would be replaced by a temperature sensor, WiFi module, and door sensor. The authors' attempt to illustrate the provided example is successful. However, these systems are excellent for individuals who want to save energy and who need a high level of security system robustness and are willing to spend more money than usual.

# Research Methodology

**Quantitative:** It involves in collecting and involving numerical data for statistical analysis (Bhandari, 2020).

In the upcoming year 2023, 10 million household decision-makers anticipate purchasing a home security system in US. This comprises 3.5 million people interested in switching or upgrading their current systems and 6.5 million new customers.

**Qualitative:** Using the information to better understand why, how, or what; qualitative data is often subjective led to certain behaviors. This paper demonstrates the ways in which Anti-theft IOT based system can be applied in the qualitative data analysis process. The basic features and primary tools of this proposed system which assist qualitative researchers in managing and analyzing their data are described.

Best approach

Based upon the analysis and gathered data, the proposed system approaches the qualitative research methodology.

While analyzing the qualitative data for home security system, a survey of various people from different backgrounds is conducted the ones who stay in different types of accommodations like a flat, home or an apartment. In this survey, it is also considered that people who have kids staying at home and/or aged parents who wish to live independently mostly feels insecure. Then an evaluation of currently installed security system is done and using that we have tried to find out different security measures adopted by the users. At the end of this survey, it is estimated to gather their opinion about advanced security system.

# Project Planning

This section of the paper discusses the system's suggested project tasks and developing the project plan. It provides a specific timeframe, usually with a schedule and stages of development that are clearly specified. It separates the process into sections like establishing quantifiable goals, deciding on deliverables, and scheduling (Lutkevich, 2021).

Chart, waterfall chart

Description automatically generated

Figure: Gantt Chart

# Conclusion

In the nutshell, IOT based home security system is simply home/office monitoring project which allows to monitor the prohibited area and the objects in real-time basis.

# References

Edwards, R., 2022. *8 Surprising Home Burglary Facts and Stats | SafeWise*. [online] SafeWise. Available at: <https://www.safewise.com/blog/8-surprising-home-burglary-statistics/> [Accessed 1 August 2022].

Saha, S., 2021. *A Bolt IoT-based Automobile Anti-theft System*. [online] Arduino Project Hub. Available at: <https://create.arduino.cc/projecthub/sahasourya/a-bolt-iot-based-automobile-anti-theft-system-57d850> [Accessed 3 August 2022].

Klein, E., 2019. [online] Logz.io. Available at: <https://logz.io/blog/the-importance-of-security-in-iot/> [Accessed 6 August 2022].

Carey, G., 2020. *The 9 Best Smart Home Security Systems of 2022*. [online] Lifewire. Available at: <https://www.lifewire.com/best-smart-home-security-systems-4034626> [Accessed 6 August 2022].

I. Gonzalez, and A. J. Caldron, “Integration of open-source hardware Arduino platform in

automation systems,” Sustainable Energy Technologies and Assessments, pp 100-557, 2014.

I. Y. Panessai, M. M. Lakulu, S. K. Subramaniam, A. F. Saad, M. I. M. Damanhuri, N. I.

Yusuf, "Developing a Prototype for Sun Tracker System Based on IoT: Controlled by Mobile

App and Online Database Monitoring," American Journal of Applied Sciences, vol. 16, no. 1,

pp. 11-25, 2019. DOI:10.3844/ajassp.2019.11.25

Lutkevich, B., 2021. *Project Planning: What is it and Steps to Create a Plan | SearchCIO*. [online] SearchCIO. Available at: <https://www.techtarget.com/searchcio/definition/project-planning> [Accessed 9 August 2022].

Castellani, A. P., Bui, N., Casari, P., Rossi, M., Shelby, Z., & Zorzi, M. (2010). Architecture and protocols for the internet of things: A case study. *2010 8th IEEE International Conference on Pervasive Computing and Communications Workshops, PERCOM Workshops 2010*, 678–683. https://doi.org/10.1109/PERCOMW.2010.5470520

Khodadadi, F., & Buyya, R. (2017). *Internet of Things: An Overview Gridbus View project Virtual Physiological Kidney View project*. https://www.researchgate.net/publication/315456657

Suresh, P., Daniel, J. V., Parthasarathy, V., & Aswathy, R. H. (2014, February 17). A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment. *2014 International Conference on Science Engineering and Management Research, ICSEMR 2014*. https://doi.org/10.1109/ICSEMR.2014.7043637

Johri, M. A. (n.d.). ADVANCE HOME SECURITY SYSTEM USING IOT.

# Risk Assessment Form

|  |  |  |
| --- | --- | --- |
| Date:8/16/2022 | Student Name: | Elisha Dhungana |
| Module: LD7022FLZ01 | Dissertation Title: An IOT based Anti-theft security system | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Item No.** | **Activity, Equipment, Materials, etc.** | | **Hazard** | | **Persons at risk** | **Severity** | **Likelihood** | **Risk Rating**  **H 20-36**  **M 12-18**  **L 1-10** | **Control Measures Required** | | | **Final Result\*** |
|  |  | |  | |  | *5* | *1* |  |  | | | *5x1=* ***5 (L)*** |
|  | Understanding the IoT frameworks and how it works. | | It leads to and software. | | Self | 5 | 2 | 6 | * Understanding the brief and history of IoT system * Literature Review | | |  |
|  | the sensor may not work for the actual system | | The possible outcomes cannot be displayed | | Self | 10 | 2 | 18 | * Proper understanding of IoT Sensors * Understanding the simulators, simulation | | |  |
|  |  | |  | |  |  |  |  |  | | |  |
| Does this Risk Assessment Require Further Specific Risk Assessment: | | | | | | | | | | | | |
|  | | | | | | | | | | | | |
| **Manual Handling: Y/N**  **Please list reference No:** | | **COSHH: Y/N?**  **Please list reference No:** | | **PUWER: Y/N?**  **Please list reference No:** | | **DSEAR: Y/N?**  **Please list reference No:** | | | | **Young Persons: Y/N?**  **Please list reference No:** | **New & Expectant Mothers: Y/N?**  **Please list reference No:** | |

**To be completed by the person undertaking the risk assessment**

Student Name: Elisha Dhungana Student ID: 21061524

Signature:

Date:88 88

Student Name: Elisha Dhungana

Student ID: 21061524 Date:8/16/2022 Signature: ELISHA

**Table

Description automatically generated**