

An IOT based Anti-theft Security System

Student Name: Elisha Dhungana

Module Code: LD7022

Module Leader: Dr. Cyril Ning Tse

Module Name: Research Methods and Dissertation Preparation

Program: MSc Web and Mobile Development Technologies

Word Count: 2256

elisha dhungana

Table of Contents

1	Aims:	2
2	Objectives:	2
3	Scope:.....	2
4	Introduction to the project:.....	3
5	Background, Motivation and Relevance 1000	4
5.1	Background Reading	4
5.1.1	Understanding of IOT:	4
5.1.2	IOT Arduino framework	5
5.1.3	IOT Raspberry Pi Framework	6
5.1.4	Key Differences between Arduino Boards and Raspberry Pi Framework.....	6
5.1.5	Technical Requirements of the System:.....	6
5.2	Motivation.....	7
5.3	Literature Review.....	7
6	Research Methodology	8
7	Project Planning	9
8	Risk Assessment	10
9	Conclusion	11
10	References.....	12
11	Appendix A.....	14
11.1	Ethics Form.....	14

1 Aims:

The aim of this proposed system is to investigate on Anti-theft IOT based Home/Office Security system and to develop a user solution application that supervises the security of the items in real-time if someone attempts to steal or changes the position.

2 Objectives:

- To study and investigate about the IOT based security system using Arduino UNO and research about the appropriate sensors to develop the actual system.
- To compare and evaluate between Arduino and Raspberry pi framework of IOT which are applicable for the design of IOT based Anti-theft Security System.
- To design a security system model that can buzz an alarm whenever someone attempts to steal or move the position of item.
- To develop and analyze the integration of mobile apps with IOT sensor using react native framework for both Android and IOS platform which can send the user an immediate SMS alert in the event of an external occurrence, such a theft.

3 Scope:

The scope of this project is to create a security system that can immediately respond to the owner or administrative department if the position of object has been changed.

The scale of this initiative is to prevent theft in private residences, jewelry stores, offices, retail establishments, and the objects in even in public places that are restricted to touch or change its position.

Arduino Uno, Wi-Fi-Shield 2 for Arduino, a force sensor, Ultrasonic sensor, a resistor, jumper wires, breadboard, camera, and buzzer are all necessary components for the system. 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 model to implement real-time **an IOT based Anti-theft Security System**.

4 Introduction to the project:

Incidents like thefts, snatching and robbery are very common these days at home, office or in any public area. The most effective deterrents system for such break-ins and burglary was only restricted to CCTV monitoring under the surveillance of human resource. Those home security system that was developed earlier that has certain drawbacks, such as being affected by power outage or the weak security. Due to this situation, intruders can be easily escape from the spot or crimes are found after being committed only. Considering those occurrences, the system is proposed as “**An IOT based Anti-theft Security System**” to provide the solution to track the intruders in real-time using the GPS tracking system and providing immediately alert to the owner/ administrative person at the time of robbery or break-ins.

The anticipated way of stealing an item or jewelry is by directly lifting from the spot. Therefore, in this proposed method, the items that needs to be secured are placed under the frame of force resistor sensor. By using force sensor, it will clearly be distinguishing the force required to pick up the item. Thus, if the detected force is higher than the threshold value of force sensing resistor, the sensor will automatically alert the owner that the item has been touched or lifted (Edwards, 2022).

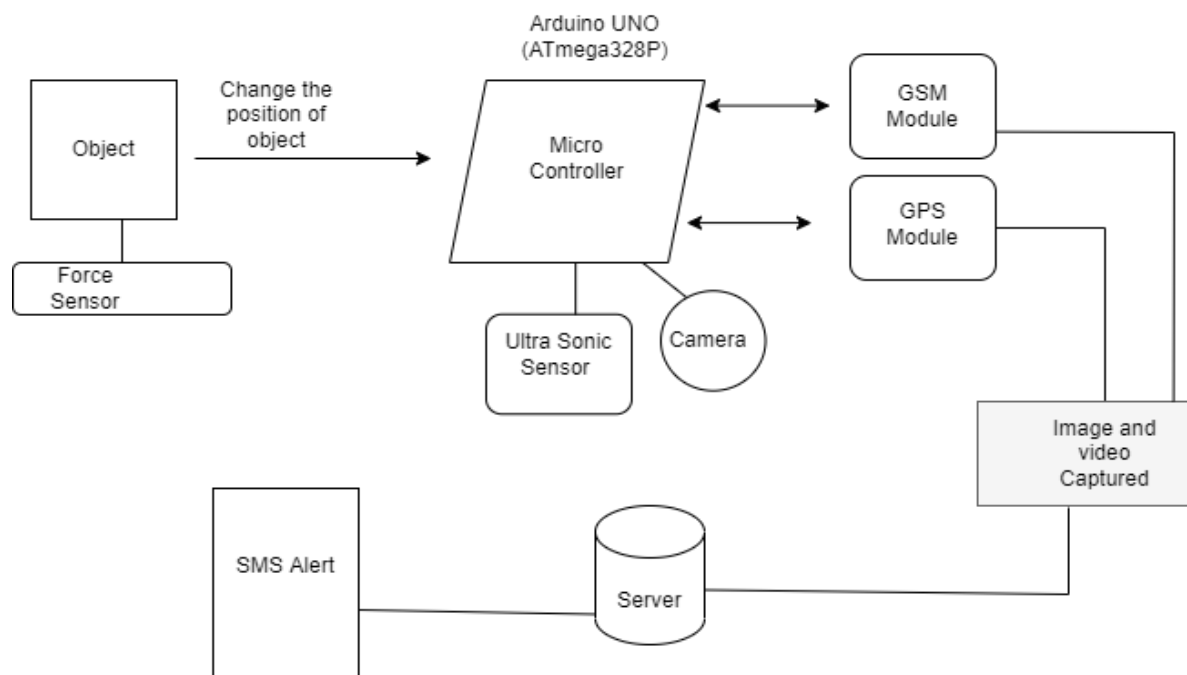


Figure 1 Architecture of An IoT Based Anti-Theft System

Figure 1 depicts the architecture of the proposed system. If the item is uplifted from the force sensor, the three level of security provided in the system are:

- IT will automatically activate the camera to camera the photos.
- It will buzz the alarm to notify people nearby.
- It will send the alert message to the owner or user.

By using the concept of IOT, the proposed system will be developed on Arduino Platform by using the technique with Arduino UNO, Force resisting sensor, buzzer to alert, camera, GPS Module, GSM module and moreover, it is done by combining sensors which is integrated to a mobile application. Thus, the project has the potential that can easily detect the intrusion and have a strong connectivity with the secure environment (Pandey et al., 2019)

It is also extremely crucial that the system be compact and simple to maintain. As a result, the proposed system includes a mobile app that controls the entire system. The system is monitored in real time by instructions obtained from applications and sensors that have been activated.

5 Background, Motivation and Relevance 1000

5.1 Background Reading

The paper is proposed to implement an **IOT based Anti-theft Security System** which is easily handled by a mobile application remotely. Furthermore, the system must be convenient and simple to maintain. As a result, the suggested system needs a lot of prior knowledge on IOT-based security systems, feasible IOT sensors, and its frameworks.

5.1.1 Understanding of IOT:

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 demand for ubiquitous context-aware platforms that support interconnected, diverse, and distributed networks of devices which is referred as 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).

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).

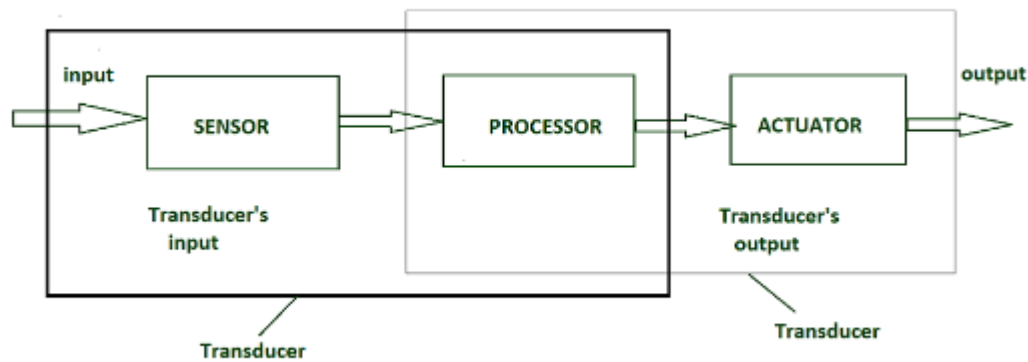


Figure 2 The working process of an IOT system (Klein, 2019)

Initially, the sensors collect the data from the environment. Connecting sensors and devices to the cloud can be achieved by using cellular, satellite, Wi-Fi, 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.

5.1.2 IOT Arduino framework

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.

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.

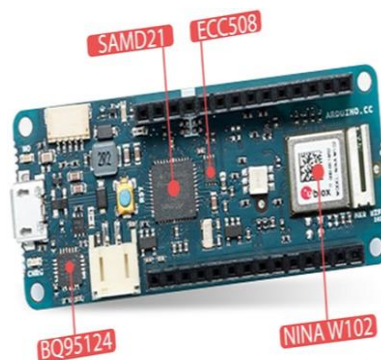


Figure 3 Arduino Device (Nesher, 2020)

5.1.3 IOT Raspberry Pi Framework

A miniature computer that can be connected to a laptop screen, keyboard, and mouse. which consists of all the characteristics of a computer, including a specialized processor and memory. It has own Raspberry Pi OS, which is an optimum version of Linux (Nesher, 2020).



Figure 4 Raspberry Pi 3 (Nesher 2020)

5.1.4 Key Differences between Arduino Boards and Raspberry Pi Framework

- Raspberry Pi boards are microprocessors, whereas Arduino boards are microcontrollers.
- The Raspberry Pi has its own operating system, whereas Arduino boards do not.
- The Arduino board operates using the instructions provided by the Arduino IDE whereas Raspberry Pi has its OS.
- Arduino board cannot be supportive the Wi-Fi whereas for Raspberry Pi can support.

5.1.5 Technical Requirements of the System:

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

5.1.5.1 Hardware Requirements

- Arduino UNO (ATmega328P)
- GPS (U-blox NEO-6M)
- GSM (SIM900A)
- Ultrasonic Sensor HC-SR04
- Force sensing resistor (FS402)
- Breadboard
- Male/Female Jumper Wires

- Buzzer
- LED
- USB-A to B Cable
- USB-A to Mini-USB Cable
- Mobile phone

5.1.5.2 *Software Requirements*

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

5.2 Motivation

The future IoT applications is vast which will be enabled through intuitive human and machine interaction. IOT enables the improved monitoring, processing, and power of entities, and products. Most of the Smart home security system employs IoT embedded products to facilitate the users to observe and manage the security of home, including access control and surveillance.

Although that were designed earlier have many limitations and drawbacks, such as not able to monitor in real-time or compromising the security. Data backup and real-time observing arrangement is necessary for security monitoring systems to minimize with the security breakdowns, early precautions can save the individuals and property items with all such consequences. The system is intended to retain such circumstances while also ensuring the security of any valuable items.

5.3 Literature Review

- Suvadeep Bose, Vishal Jain, and Ravi Kishore proposed an IOT model that focuses on designing wirelessly home security systems that alert the operator through the Internet in case of trespass and alternatively raises an alarm (Ravi et.al,2019).
- K. Hemasaisiva prasad et al.(2016) has proposed structure that assures the creation of an innovative anti-theft ATM system. 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 on Security Design and Implementation intended for Smart Homes Using GSM Expertise, 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. Although the cameras are cost-effective, 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.

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

6 Research Methodology

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 An IoT based Anti-theft system can be applied in the qualitative data analysis process.

Based upon the main idea, purpose, study and required data, the proposed system approaches the qualitative research methodology.

The basic features and primary tools of this proposed system which assist qualitative researchers in managing and analyzing their data are described.

1. User Interview, questionnaires, and observation method

User interviews are one of the qualitative research methods in which a user is simply asked a question and the responses are recorded and reported for further discussion. In these discussions, 4-5 number of public users can be interviewed and analyze the data according to the response.

2. Focus Group Discussions:

This focus group discussion method will be used to collect data from people with similar backgrounds or practices who have come together to discuss about the same topic such as: Existing Home Security System, IOT based item tracking system and so on. The main purpose of this group discussion is to understand the desire of local people about security based IOT system that they may need at their place.

3. Documentation Review, Case studies, community mapping

This method of research included the background reading of similar existing system, going through the case studies and identifying the people who are seeking such kind of assistance or actual system.

4. Preparing System Requirement Specification (SRS) Document

While preparing SRS document, a description of functional and nonfunctional requirements should include.

7 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).

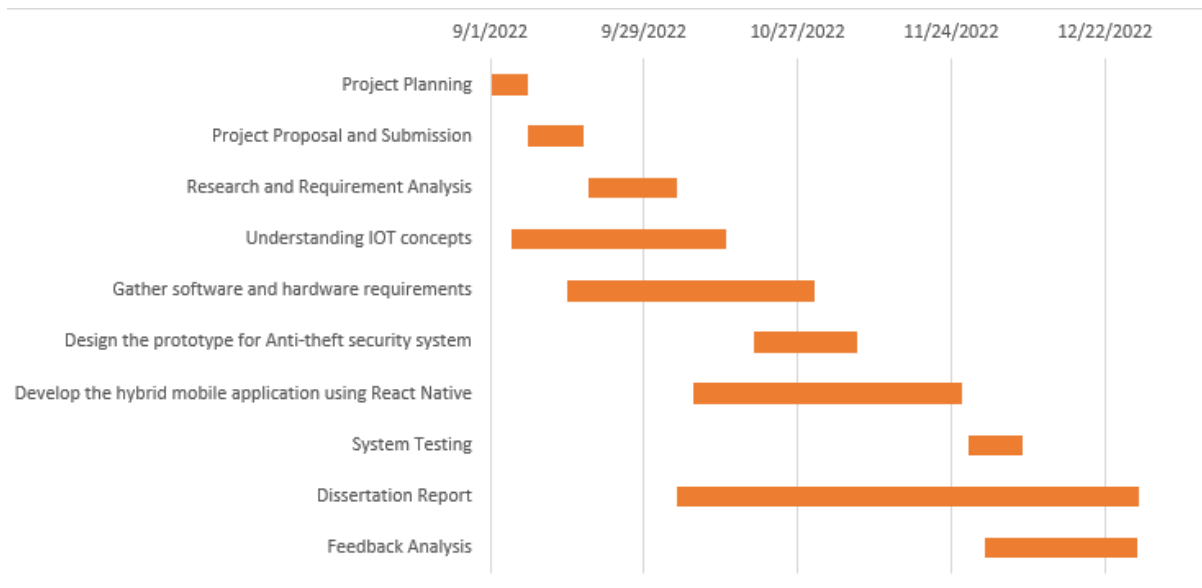


Figure 5 Gantt Chart

From the figure 5, it determines that the estimated start date of proposal is 9/1/2022 and end date is 12/22/2022.

8 Risk Assessment

There are certain risks that are associated while developing the system such as Understand the concept of IoT and choosing the appropriate framework to develop the system. The most challenging risk that I found is to deal with connectivity and compatibility issue of IoT sensor.

It is depicted in the following form what are the possible risks and how it can be controlled with the risk ratings.

Item No.	Activity, Equipment, Materials, etc.	Hazard	Persons at risk	Severity	Likelihood	Risk Rating	Control Measures Required	Final Result*
						H 20-36 M 12-18 L 1-10		
1.	Understanding the IoT framework and choosing the best approach.	Choosing the appropriate approach or framework of IOT becomes a challenge to get into the right track to design and develop the system.	Self	4	2	8	<ul style="list-style-type: none"> Understanding the brief about IOT system and comparing each framework in terms of the connectivity and security. Background reading and examining the published papers that are related to proposed system. 	8
2.	Gather the IOT sensors and hardware requirements.	Purchasing and gathering appropriate the IoT sensors, buzzer, microcontroller can be challenging.	Self	2	2	4	<ul style="list-style-type: none"> Proper collection of appropriate IoT Sensors before the initiation of system development 	4
3.	Integration of IOT device with mobile	Integration of IoT device with cross-platform for	Self	5	1	5	<ul style="list-style-type: none"> Proper research on development process of hybrid mobile application 	10

	application.	both Android and IOS application can be challenging.					and learning react native to develop for both android and iOS device simultaneously.	
4.	Deal with connectivity and compatibility issue of an IOT sensor.	The possible outcomes cannot be displayed.	Self	5	3	15	<ul style="list-style-type: none"> Putting additional effort in design and development of system in simulator using Arduino IDE or wokwi.com 	15
Does this Risk Assessment Require Further Specific Risk Assessment: NO								
Manual Handling: Y/N? Please list reference No: NO		COSHH: Y/N? Please list reference No: NO	PUWER: Y/N? Please list reference No: NO	DSEAR: Y/N? Please list reference No: NO		Young Persons: Y/N? Please list reference No: NO		New & Expectant Mothers: Y/N? Please list reference No: NO

9 Conclusion

In the nutshell, An IOT based Anti-theft Security System is simply monitoring project which allows to prevent the theft from home, office or any store and the objects are monitored real-time using the GPS.

The application must comply to the Data Privacy Notice and GDPR regulation while the hybrid mobile application development phases must meet the criteria to W3C standards identifying the key requirements and guidelines for the optimization and accessibility criteria.

Moreover, to realize the legal and ethical aspects of the mobile application and the IOT project in a proper way, it is necessary to follow the guidelines from British Computer Society (BCS).

Many critical issues that may arise during development and testing can have an impact on the actual business model of any organization, regardless of its legal, political, or cultural circumstances. As a result, rather than being addressed throughout the software development process, these issues must be addressed at the level of business ethics.

10 References

- Bhuvaneswari, V., & Porkodi, R. (2014). The internet of things (IOT) applications and communication enabling technology standards: An overview. *Proceedings - 2014 International Conference on Intelligent Computing Applications, ICICA 2014*, 324–329. <https://doi.org/10.1109/ICICA.2014.73>
- 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].
- 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>
- 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].
- 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
- Khodadadi, F., & Buyya, R. (2017). *Internet of Things: An Overview Gridbus View project Virtual Physiological Kidney View project*. <https://www.researchgate.net/publication/315456657>
- Klein, E., 2019. [online] Logz.io. Available at: <<https://logz.io/blog/the-importance-of-security-in-iot/>> [Accessed 6 August 2022].
- 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].
- Nagamani, T., Beniga, W. H., Dhanish, K. S., & Sherine Benitta, A. (2022). *Anti-Theft Monitoring for a Smart Home*. 76–82. <https://doi.org/10.1109/icssit53264.2022.9716311>
- Nesher, G., 2020. IoT Development with the Raspberry Pi. [online] InfoQ. Available at: <<https://www.infoq.com/news/2020/01/raspberry-pi-iot-with-javascript/>> [Accessed 22 August 2022].

Pandey, S., Gupta, S., Saxena, S., & Tyagi, D. (2019a). *Smart Home Security System using IOT*. <https://doi.org/10.5281/zenodo.2709387>

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].


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*

11 Appendix A

11.1 Ethics Form

Submission

Submission Ref 53024
Status New
Submission Coordinator

Name  elisha.dhungana

Email elisha.dhungana@northumbria.ac.uk

Faculty

Department

Submitting As

Externally Approved ☐ Note: ONLY tick this box if your project has already received full ethical approval from an external organisation

Module Level Approval ☐ Tick this box if staff and this submission refers to an entire module.

**** Only to be used for low or medium risk projects as categorised by the diagnostic risk question set ****

Module Code

[Help](#)

Module Tutor

[Find](#)

[Help](#)

[Clear](#)

Titl... Programme Leader

Dep... Vice Chancellors Office

Em... ning.tse@northumbria.ac.uk

Named Submission Coordinator (PGT/UGT only)

Find

Help

Clear

If you are an undergraduate or postgraduate taught student please select a Named Submission Coordinator. If you are not sure who this is please contact your Module tutor or Supervisor as appropriate.






Ethical Risk Level

Low

Click here to answer the ethical risk questions

Ethical Risk Diagnostic Questions and Responses		
<div>Refresh</div>		
ID	QUESTION	ANSWER
1	Gathering data or information from human participants (e.g. via questionnaire / interview/survey/experiment/ social media/ VR)?	NO
2	Collecting personal data, i.e. name, email, home address, computer IP address, phone number etc?	NO
3	Analysis of secondary data NOT in the public domain (e.g. archive material that require organisational membership)?	NO
4	The collection or use of information which is ‘commercially sensitive’?	NO
5	Financial inducements other than expenses and compensation for time?	NO
6	Gathering data/information at a physical location external to Northumbria University campuses, franchised locations, and not your normal place of work?	NO
7	Collection of samples such as plants, soils etc, that might disturb the environment or archaeological remains?	NO
8	Research involving animals or materials derived from animals?	NO
9	Anything else which means that the research poses greater than minimal ethical risk?	NO

Co-investigators

 Add  Edit  Delete  Save  Refresh

NAME OF CO-INVESTIGATORS

No items to display.

G1: General Aims and Research Design (Mandatory)

Title

Title of your research project

An IOT based Anti-theft Security System

Outline General Aims and Research Objectives

State your research aims/questions (maximum 500 words). This should provide the theoretical context within which the work is placed, and should include an evidence-based background, justification for the research, clearly stated hypotheses (if appropriate) and creative enquiry.

1 Aims:

The aim of this proposed system is to investigate on Anti-theft IOT based Home/Office Security system and to develop a user solution application that supervises the security of the items in real-time if someone attempts to steal or changes the position.

2 Objectives:

- To study and investigate about the IOT based security system using Arduino UNO and research about the appropriate sensors to develop the actual system.
- To compare and evaluate between Arduino and Raspberry pi framework of IOT which are applicable for the design of IOT based Anti-theft Security System.
- To design a security system model that can buzz an alarm whenever someone attempts to steal or move the position of item.
- To develop and analyze the integration of mobile apps with IOT sensor using react native framework for both Android and IOS platform which can send the user an immediate SMS alert in the event of an external occurrence, such a theft.

G2: Research Activities (Mandatory)



Please give a detailed description of your research activities

Please provide a description of the study design, methodology (e.g. quantitative, qualitative, practice based), the sampling strategy, methods of data collection (e.g. survey, interview, experiment, observation, participatory), and analysis. Do sensitive topics such as trauma, bereavement, drug use, child abuse, pornography, extremism or radicalisation inform the research? If so have these been fully addressed?

QUALITATIVE including interview, group discussions, surveys.

G3: Research Data Management Plan (Mandatory)



Anonymising Data (mandatory)

Describe the arrangements for anonymising data and if not appropriate explain why this is and how it is covered in the informed consent obtained.

There is no anonymising data in the project

Storage Details (mandatory)

Describe the arrangements for the secure transport and storage of data collected and used during the study. You should explain what kind of storage you intend to use, e.g. cloud-based, portable hard drive, USB stick, and the protocols in place to keep the data secure.

If you have identified the requirement to collect 'Special category data', please specify any additional security arrangements you will use to keep this data secure.

The data will be stored in the G0oogle CCloud Platform.

Retention and Disposal (mandatory)

☒ I confirm that I will comply with the University's data retention schedule and guidance.

[Research Data Management link](#)

[General Data Protection Regulations including Data Protection link](#)

[Records Retention Schedule link](#)

G4: Research Project Timescale (Mandatory)

Proposed Start Date

01/09/2022



Proposed End Date

31/12/2022



G5: Additional Information

☐ Externally Funded

External Funder



Please give details of your 'other' funder

Agresso Reference

☐ Franchise Programme Organisation

Please give details of your franchise organisation

Type a value

☐ NHS Involvement

Please give details of any NHS involvement

Type a value

☐ Clinical Trial(s)

Please give details of any Clinical Trial(s)

Type a value

☐ Medicinal Products

Please give details of any Medicinal Product(s)

G6: File Attachments



Additional files can be uploaded e.g. consent documentation, participant information sheet, etc.

Please note: It is best practice to combine all documents into one PDF (This avoids the reviewer having to op...

Go To Attachments

G7: Health and Safety (Mandatory)



☒ I confirm that I have read and understood the University's Health and Safety Policy.

☒ I confirm that I have read and understood the University's requirements for the mandatory completion of risk assessments in advance of any activity involving potential physical risk.

The University Health and Safety Policy can be accessed [here](#)

The University Risk Assessment Code of Practice can be accessed [here](#)

Please confirm either:

☐ There are PHYSICAL risks associated with the research project work and I confirm that a risk assessment has been approved and attached to this ethics submission.

OR



I can confirm that there are no physical risks associated with this project and so no risk assessments are required.

Students requiring assistance with completing their risk assessment should get in touch with their supervisor or module tutor as the first point of contact. If further assistance is needed, the Faculty Technician can provide further guidance.

For more specific risk assessments (e.g. lab work), especially where the project is Medium or High risk, you are required to consult the Faculty Technical Manager; your Supervisor/Module Tutor will be able to put you in touch.

If you have any questions or concerns, please contact the University Health and Safety Team by emailing

CRHealthandSafety@northumbria.ac.uk

G8: Insurance (Mandatory)



I have read and understood the University Insurance guidance document (link below):

[Insurance Guidance link](#)

If you think your activity may involve a High Risk rating or are unsure how to answer the statements - contact fi.insurance@northumbria.ac.uk with a copy of your research proposal for advice.

I confirm my work is covered by University Insurance. I confirm an insurance risk level of:

Low



If your insurance risk level is HIGH please attach details of exceptional insurance coverage:

Click here to attach a file

G9: Electronic Signature (Mandatory)



I confirm my supervisor has reviewed the contents of this document



I confirm I have assessed the ethical risk level of my work correctly and answered the above

sections as fully and accurately as possible.

Full Name

elisha.dhungana

Date

22 August 2022 12:54:12



PDF Version



Create PDF

No items to display.

Log of any Ethical Incidents



Log New Incident

INCIDENT...	CREATED DATE TIME	CREATOR NAME	COMPLAINANT DETAILS
-------------	-------------------	--------------	---------------------

No items to display.

Title and Objectives (see G1)



+ Add



Save

Reviewer A:



Reviewer B:



e.g. Are the research question and/or study aims clear?

DATE

ROLE

COMMENT

No items to display.

Proposed Methodology and Analysis (see G2)



+ Add



Save

Reviewer A:



Reviewer B:



e.g. Is the design appropriate to the research question?
Are the methods of data analysis appropriate to the research question?

DATE	ROLE	COMMENT
------	------	---------

No items to display.

Sample and Recruitment (see M1)

+ Add Save

Reviewer A:

Reviewer B:

e.g. Is the sampling approach appropriate to the design?
Is the sample sufficient and achievable?
Is the process of recruitment clearly explained?
Are participants receiving payments for taking part, and if so is the payment appropriate?
If the DBS is ticked, has the appropriate information been included?

DATE	ROLE	COMMENT
------	------	---------

No items to display.

Consent (see M1)

+ Add Save

Reviewer A:

Reviewer B:

e.g. Is the approach to consent seeking clear?
Is consent from parents/ carers/ guardians required?
Are all necessary recruitment and informed consent documentation included (e.g. letters of permission, letters of invitation)
Is the information sheet adequate to ensure informed consent?
Are the consent form(s) appropriate?

DATE	ROLE	COMMENT
------	------	---------

No items to display.

Researcher and Participant Safety (see M1)

+ Add
Save

Reviewer A:
Reviewer B:

e.g. Is there any risk of physical harm for the researcher(s) or the participants and if so what attempts have been made to alleviate or minimise them?
Have Risk Assessments been referred to where appropriate?

DATE	ROLE	COMMENT
No items to display.		

Research Activities (see G2-G8, M1-M5, H1-H5)

+ Add
Save

Reviewer A:
Reviewer B:

e.g. Are the research tasks described clearly?
Do sensitive topics such as trauma, bereavement, drug use, child abuse, pornography or extremism/ radicalism inform the research? If so have these been fully addressed? (and we can use this to amend the information on risk levels on the form)Is there any risk that the tasks may cause psychological harm and if so what attempts have been made to alleviate or minimise them?

DATE	ROLE	COMMENT
No items to display.		

Data Management Plan (see G3)

+ Add
Save

Reviewer A:
Reviewer B:

e.g. Have sufficient steps been taken to ensure participant anonymity/confidentiality of data?
Are the arrangements for data storage and disposal clearly outlined?
Are these arrangements in line with University and/or the funding body requirements?

DATE	ROLE	COMMENT
No items to display.		

File Attachments (see G6)

Add

Save

Reviewer A:

Reviewer B:

Please note: where file attachments have not been added because they are not required, please select Approve.

COMMENT BY	DATE	ROLE	COMMENT
No items to display.			

General Comments (see Help)

Add

Save

Help

DATE	ROLE	COMMENT
No items to display.		

25 | Page