



Sri Lanka Institute of Information Technology

MisplaceX-IT device detection and monitoring system in office environments

Project proposal report

Project ID: 23-345

Student registration no: IT20028046

S.B.M.B.S.A Gunathilaka

Date of submission: 05th May 2023

DECLARATION

We confirm that we worked hard on this document and didn't copy it from anyone else. It's completely original and hasn't been submitted elsewhere before, not outside the university.

Name	Student ID	Signature
S.B.M.B.S.A Gunathilaka	IT20028046	<i>Buddhika.</i>

ABSTRACT

Conventional approaches to tracking and managing IT assets can be time-consuming and prone to human mistakes, such as manual inventory management or barcode scanning. Therefore, there is a demand for automated and more effective solutions. Although this issue might be solved using image processing technologies, no studies have been done on this particular usage. Cameras could be put in server rooms or data centres with image processing to track the whereabouts and motion of IoT assets. It might be able to automatically track each item's position and spot any theft or misplacing instances by utilizing algorithms to evaluate the images taken by these cameras. The issue is that managing and securing IT assets in office contexts lacks practical, cost-effective solutions. This increases the possibility of asset theft, loss, or misplacement, which could be harmful to business operations. Although image processing technology may be able to solve this issue, more investigation and development are required to make it a workable and feasible solution.

Keywords - IT assets, image processing, data centres, IoT, algorithms, cost-effective, asset theft

CONTENT

DECLARATION	2
ABSTRACT.....	3
INTRODUCTION	6
Background & Literature Survey	6
Research Gap	8
Research problem	10
OBJECTIVES	11
Specific Objectives	12
METHODOLOGY	15
System architecture	15
Design.....	16
Component overview diagram	17
Description of Personal and Facilities.....	17
GANTT CHART	19
WORK BREAKDOWN STRUCTURE	19
PROJECT REQUIREMENTS	20
Functional requirements.....	20
Non-functional requirements	20
User requirements	21
Budgetary Plan.....	22
Commercialization	22
Target Audience	22
Market Space	23
References	23
APPENDIX.....	24
SIMILARITY REPORT	24

LIST OF FIGURES

Figure 1: System Overview Diagram	15
Figure 2: Individual component diagram.....	17
Figure 3: Gantt Chart	19
Figure 4: Work Breakdown Chart	19
Figure 5: Turnitin similarity report.....	24

LIST OF TABLES

Table 1: Individual component gap with existing systems	9
Table 2: personal and facilities	18
Table 3: Budget	22

INTRODUCTION

Background & Literature Survey

Due to the widespread use of mobile devices and the rise in remote work, companies are encountering fresh obstacles when it comes to safeguarding their data. Of particular concern is unauthorized electronic equipment within company premises - this insidious presence has the potential to undermine organizational networks and breach confidentiality measures. There has been a surge of interest lately in devising solutions that can track unapproved hardware brought into office spaces so as protect against security breaches."Real-time device monitoring in the workplace has been the subject of numerous research projects. A system that employs BLE beacons and machine learning methods to recognize and monitor devices in the office environment was suggested by Kim et al. (2017) in one study. The system was put to the test in a real office setting, and it was discovered to be efficient at spotting devices and sending out alerts when unauthorized devices were spotted.

In another study, Hwang et al. (2019) suggested a system that uses camera-based image processing algorithms to detect and monitor gadgets in real time. The system was tested in a laboratory environment and was shown to be effective at detecting and tracking gadgets. The technology also issued alarms when unauthorized devices were discovered. In addition to real-time device monitoring, there has also been a study on establishing systems that can control the access of devices to the office environment. One option is to utilize whitelist and blacklist policies, where devices are allowed or refused access, depending on established policies. In a study by Basnet et al. (2018), a system was proposed that used machine learning algorithms to understand the patterns of device usage in the office setting and generate policies for device access control. Another way is to utilize device fingerprinting techniques to detect and authenticate devices. In a study by Shah et al. (2017), a method was proposed that used a combination of hardware and software-based techniques to produce unique device fingerprints for authentication. The system was tested in a laboratory environment and was proven to be effective in recognizing and authenticating devices.

Location tracking systems have also been offered as a technique for identifying misplaced or lost gadgets in the working setting. In a study by Zhang et al. (2019), a system was proposed that used RFID tags and position triangulation techniques to locate misplaced gadgets in the office setting. The system was tested in a laboratory environment and was shown to be effective at locating gadgets. In light of the rising use of mobile devices and remote work, real-time device monitoring and access control solutions are essential for assuring the security of office settings. Effective monitoring and control systems can be created with the use of technologies like BLE beacons, camera-based image processing, machine learning, device fingerprinting, and location tracking. To address issues including privacy concerns, scalability, and interoperability with current systems, more study is required in this field.

Research Gap

In the last year, this image processing technology usage has been raised for applications such as face mask detection with the pandemic situation. and since before the pandemic, most organizations have used facial recognition to give access to employees to their facilities and office areas. There is less number of researchers that have done similar to our research. Here are some of them and what are the newly added things in our research.

There is research [1] done that uses Wi-Fi signals to manage end-user devices based on their current location, and it allows the admin to see where the end-user devices are currently. The authors say that traditional device management systems are not enough, so they create this system to manage devices with the help of Wi-Fi technology. But there are some issues with this system that are addressed by our research. We planned to locate devices not using Wi-Fi but using other technology like Bluetooth and RFID. because if the end-user device is switched off or it has separated from other units, then our system is still able to locate them. Also, we planned to integrate with video surveillance systems that allow identifying devices through video footage.

Another research [2] was done with the help of ultra-wideband (UWB) technology for real-time tracking and localization of multiple devices. This technology is great for big ranges, but it has a few problems, such as higher power consumption, lack of indicators when we near the device, and there no mapping system .to address that, we have added indicators such as LEDs, buzzers for our hardware module and we are going to build a mapping mechanism that helps to identify where the device is currently in the office.

Most of the research tends to use Bluetooth technology such as [3] .in this research, they have created a system using BLE beacons that allows them to receive signals from the devices using low-energy Bluetooth signals. It has low battery consumption and is great for small indoor areas. But in our case office environment is a little bit larger indoor area, so only depending on Bluetooth technology is not enough. So we are not only concerned about battery consumption, we need a larger range. We use a combination of location-tracking technologies to get better performance in larger and shorter ranges.

In addition to that, we consider incorporating machine learning algorithms to improve the accuracy of device tracking or integrating the system with a desktop application for device

monitoring and management. Additionally, you could explore the use of alternative sensors or technologies for device tracking, such as ultrasound or infrared sensors.

There are more existing studies done on the topic of “locating misplaced devices”.

- (A) ZigBee-based positioning system [4].
- (B) Bluetooth-based approach for locating misplaced objects [5].
- (C) UWB-based wireless sensor network for locating misplaced objects [6].
- (D) An indoor localization and tracking system based on ultra-wideband technology [7].

The novelty of our proposed work

- Use of both UWB and GPS technologies.
- Integration with an Arduino board.
- Integration with a map of the office.
- switch to GPS mode if a misplaced device is not in the UWB range.
- specifically designed for use in critical office areas.

Features	(A)	(B)	(C)	(D)	Ours
Applicable for short ranges	✓	✓	✓	✓	✓
Applicable for long(outdoor) ranges	✗	✗	✗	✗	✓
Use of UWB technology	✗	✗	✓	✓	✓
Build for critical office areas	✗	✗	✗	✗	✓
penetrate walls and obstacles	✗	✗	✓	✓	✓

Table 1:Individual component gap with existing systems

Research problem

When we come to the environments such as offices, there are so many sections and work areas, and there is so much electronic equipment, and most of them are IOT devices such as desktops, laptops, keyboards, routers etc. these devices are used for various types of operational tasks by employees in their workstations. According to the task, these devices are assigned to employees, teams and departments to get efficient output. In some scenarios, employees have to borrow other devices from other departments, or they have to bring their devices to other departments according to their tasks. Therefore, there is a risk of misplacing devices, or if the devices are exactly the same, they can be exchanged between departments while they don't aware of that, or even a theft can happen within the office.

There are mechanisms, such as most organizations maintaining a table that mentions the employee ID and the device's serial number that has been assigned to a particular employee, but that really works for the computing devices such as laptops and desktops. Other than that, it's not effective for other devices. This is the place we need to have a device inventory and track them in the office environment. This device inventory should have a proper mechanism to maintain data, and those data should be very accurate. This is a big challenge in office environments because they have to use thousands of devices in the office. Inaccurate or incomplete device inventories can lead to lost productivity, security risks, and increased costs for the organization. And also Misplaced or stolen devices can also pose significant security risks, as sensitive data stored on these devices can be accessed by unauthorized individuals.

To solve these problems, we propose a system that can identify and detect the physical behaviour of a workstation, and this workstation can be a critical one, such as a workstation in a data centre or server room. Then our system can detect if one of the devices is misplaced or if the arrangement of the devices has changed without the user's awareness. For that, we have to use image processing techniques such as object detection and recognition to identify devices on a workstation. Then we give the necessary data with a dataset that needs to the system to identify if there is something suspicious happened.

Previous research has explored the use of various technologies for device tracking and management, such as RFID, Bluetooth, and Wi-Fi signals. However, these technologies have limitations, such as limited range and accuracy, which can affect their effectiveness in an office environment. In our research, we are planned to use a combination of technologies to obtain accurate results and give more features to the system admin to use whenever he needs.

OBJECTIVES

monitor devices in an office setting and quickly identify any that don't belong or are missing. The system should use image processing to evaluate real-time photographs of the workspace, and an Arduino or Raspberry Pi module will help with this. If an unauthorized device is detected or a device is missing from its assigned location, an alarm should sound to alert employees. The goal is to improve workplace security and prevent device loss or theft.

Specific Objectives

To achieve the main objective, we have to come up with the below specific objectives.

Implement a real-time monitoring system for devices in an office environment that gives alerts for unauthorized or missing devices.

- Installing and setting up image processing software or libraries such as OpenCV
- Capturing images or video of the office environment at regular intervals Implementing algorithms for detecting and recognizing devices in the captured images or video
- Storing information about authorized devices and their intended locations in a database
- Creating rules for device monitoring, such as determining which devices should be monitored and what actions should be taken when a device is found to be out of place.
- Implementing an alert system for sending notifications to the relevant parties when a device is missing or out of place.
- Testing and fine-tuning the image processing algorithms to ensure accurate device detection and recognition.

Create an interface and process the data

- Whitelist creation: Develop a mechanism for users to inform the system admin and add their devices to the whitelist, ensuring that only authorized devices are allowed in the office environment.
- Access control: Implement a system to control access to devices based on the whitelist. If a device is not on the whitelist, the system should identify it as an unauthorized device and block access.
- Integration with other components: Integrate this module with the real-time monitoring and alerting component, the device access management component, and the security component.
- Logging and reporting: Implement a system to log and report on device access attempts and other relevant events. This should include the ability to generate reports and send logs to SIEM servers.
- Blacklist creation: Develop a mechanism for blacklisting devices that have been removed from the office environment to prevent unauthorized access.
- Device matching: Ensure that the device capabilities match the organization's policies, which could involve setting specific permissions or restrictions for each device.

- User interface development: Design and develop a user-friendly interface for users to interact with the system and manage their devices.
- Integration with the system: Integrate this component with the real-time monitoring and alerting component, the location tracking component, and the security component to provide a seamless and integrated solution.
- Testing and validation: Test and validate the component to ensure that it accurately and reliably manages devices and integrates seamlessly with the rest of the system.
- Documentation: Document the design and implementation of the component to ensure that other team members and future developers can understand and maintain the system.

Build a module that can locate misplaced devices.

- Hardware setup: select the appropriate hardware components, such as a microcontroller board (Arduino or Raspberry Pi), sensors, and communication devices (Wi-Fi, Bluetooth, etc.), and assemble them into a working system.
- Software development: write the software code to control the hardware components, including reading sensor data, processing and analysing data, and communicating with other parts of the system.
- Location tracking: develop algorithms and techniques to track the location of devices within the office environment. This may involve using techniques such as triangulation, RFID, or BT signal strength.
- Integration with the system: integrate this module with the rest of the system, including the real-time monitoring and alerting component, the device access management component, and the security component.
- Testing and validation: it is important to test and validate the module, making sure it accurately and reliably tracks the location of devices and integrates seamlessly with the rest of the system.
- Documentation: document the design and implementation, including hardware schematics, software code, and algorithms, to ensure that other team members and future developers can understand and maintain the system.
- Maintenance and support: need to provide ongoing support and maintenance for the module, including fixing bugs, updating the software and hardware, and addressing any issues that arise in production.

Check user availability in critical workstations and generate alerts according to response and Bluetooth tracking.

- User activity monitoring: Implement a mechanism to monitor and track user activity on their devices within the office environment. This may involve capturing keystroke logs, mouse clicks, and other metrics that can help determine whether a device is in use.
- Vulnerability detection: Develop algorithms and methods to detect when a user has forgotten to lock their computer and leave their seat. This may involve monitoring screen activity, keyboard usage, and other metrics.
- Unusual activity investigation: If unusual activity is detected by the security operation centre, the system should be able to investigate it and provide relevant information to help identify the cause of the issue. This may involve retrieving logs, analysing network traffic, and using other techniques to gather data.
- Integration with security operations centre: Integrate the system with the security operation centre so that alerts and notifications can be sent to the appropriate personnel.
- Reporting: Develop a reporting mechanism to provide relevant information and data to the security operations centre, including logs, activity metrics, and other relevant data.

METHODOLOGY

System architecture

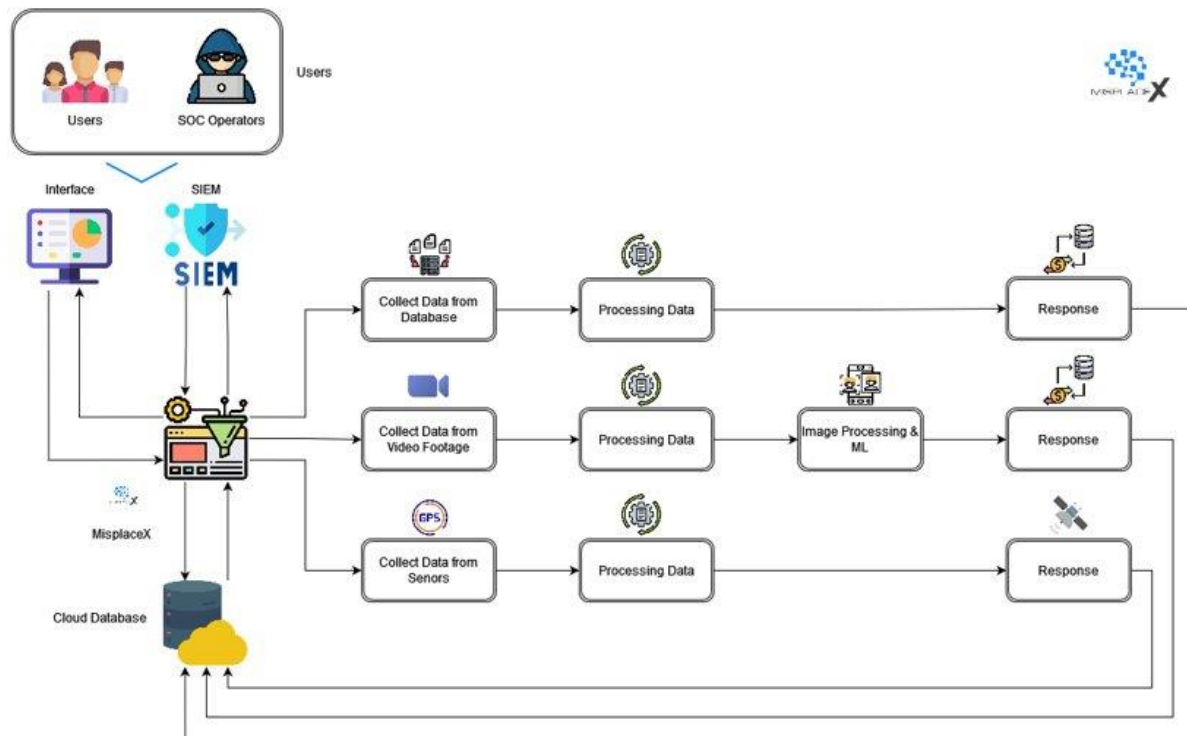


Figure 1: System Overview Diagram

With our system, we'll employ a video camera to record the workplace setting, and an image processing unit will examine the recorded video. The image processing unit will recognize the office equipment in the video and provide the information to an algorithm that was created to control the office equipment. The dataset and the beginning data are the two inputs needed for this approach.

The first data will contain specifics about the sorts of devices that should be present in the workplace as well as the planned device placement in the workstation. To gather specific information about the devices, such as whether they are authorized or barred from entering the office and their unique features, the algorithm will connect with the device database.

The algorithm will identify when a device has been misplaced or is not in its intended location and utilize data from the location tracking module to establish the device's current position. The administrator may visit the system's application interface to examine a list of the devices that are permitted or rejected for usage in the workplace, along with data about each one's characteristics. The admin will also be able to add or delete devices from the allowlist or denylist using the software.

The administrator will also be able to view the real-time position of the missing devices via the application interface. This solution will make it simpler to manage devices in the office, make it quicker to identify lost devices, and block unauthorized devices from entering the premises.

Design

It is crucial to comply with industry standards and thoroughly examine the relevant field's system when creating a proposed system. This stage plays a significant role in the system's evolution. The conceptual architecture of the system is derived from the system analysis and later translated into a physical design. During the design stage, the programming language, hardware-software platform, input, output, and database are all detailed. The data layout, method of control, data source, workload, and device restriction setup, along with documentation, tests, system implementation process, and backups, are also explained at this point.

OVERVIEW DIAGRAM

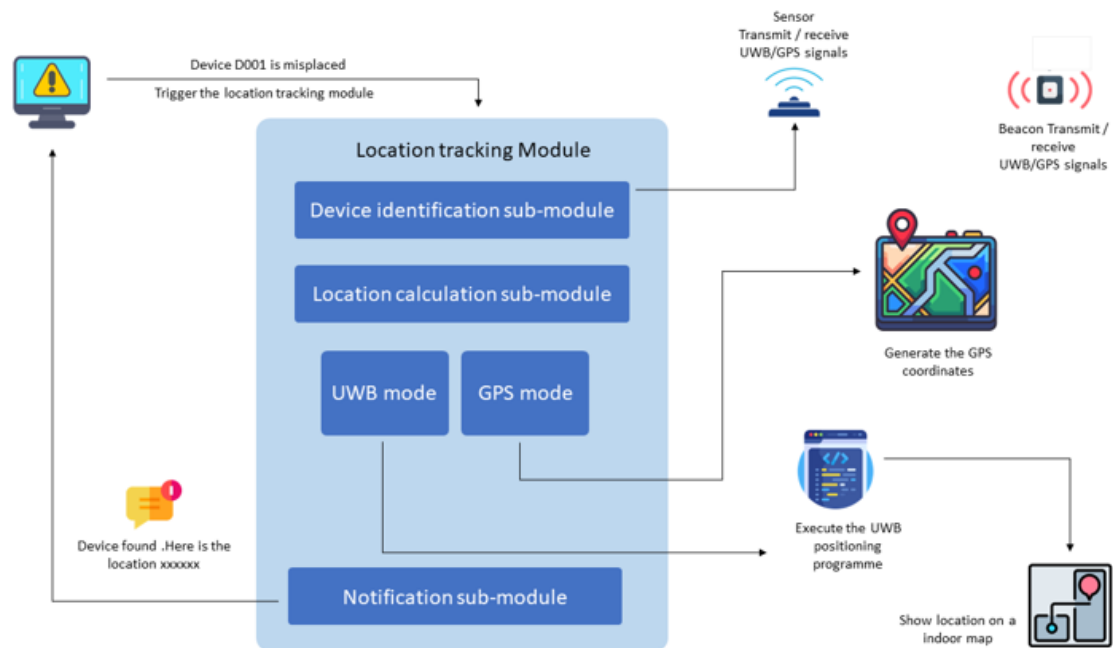


Figure 2:Individual component diagram

Description of Personal and Facilities

Name	Component	Task
Gunathilaka S.B.M.B.S.A	Build a module that can locate misplaced devices	<p>Hardware setup: select the appropriate hardware components, such as a microcontroller board (Arduino or Raspberry Pi), sensors, and communication devices (Wi-Fi, Bluetooth, etc.), and assemble them into a working system.</p> <p>Software development: write the software code to control the hardware components, including reading sensor data, processing and analyzing data, and communicating with other parts of the system.</p>

		<p>Location tracking: develop algorithms and techniques to track the location of devices within the office environment. This may involve using techniques such as triangulation, RFID, or BT signal strength.</p> <p>Integration with the system: integrate this module with the rest of the system, including the real-time monitoring and alerting component, the device access management component, and the security component.</p> <p>Testing and validation: it is important to test and validate the module, making sure it accurately and reliably tracks the location of devices and integrates seamlessly with the rest of the system.</p> <p>Documentation: document the design and implementation, including hardware schematics, software code, and algorithms, to ensure that other team members and future developers can understand and maintain the system.</p> <p>Maintenance and support: need to provide ongoing support and maintenance for the module, including fixing bugs, updating the software and hardware, and addressing any issues that arise in production.</p>
--	--	---

Table 2:personal and facilities

GANTT CHART

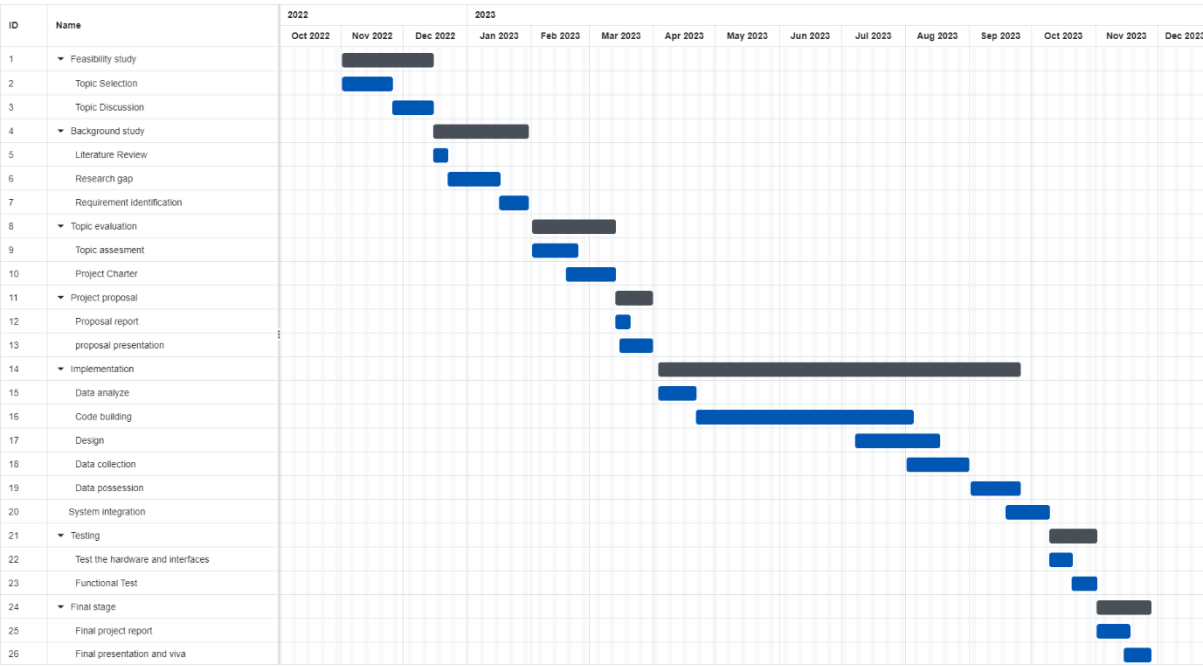


Figure 3:Gantt Chart

WORK BREAKDOWN STRUCTURE

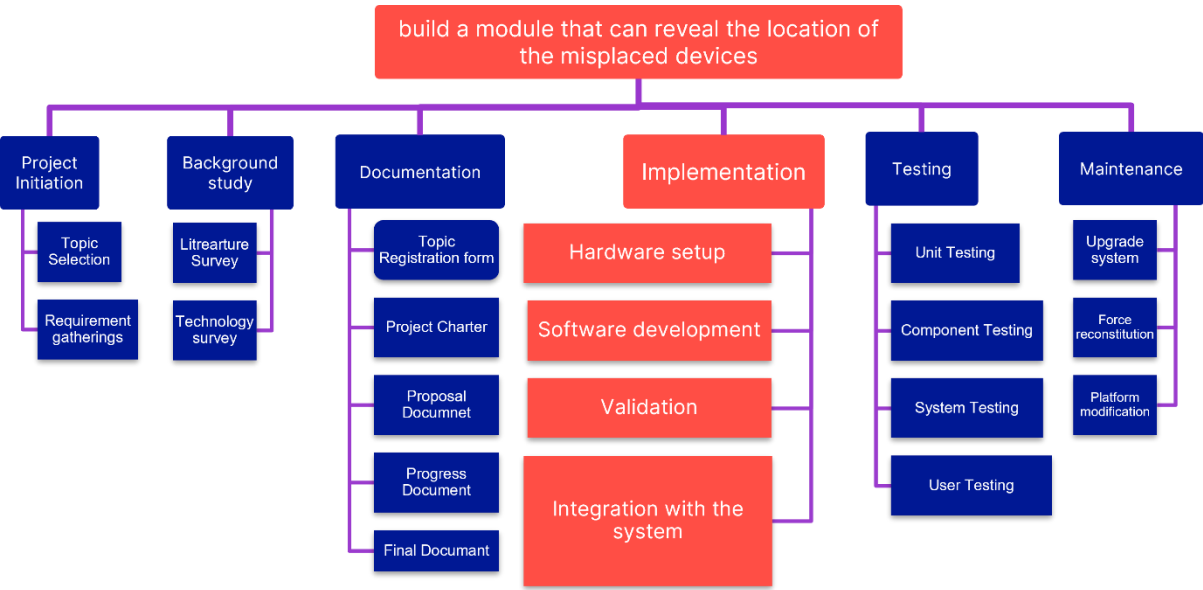


Figure 4:Work Breakdown Chart

PROJECT REQUIREMENTS

Functional requirements

- Device recognition: The system must accurately identify and catalogue devices in the workstation using video input.
- Device arrangement tracking: The system should track the arrangement of devices and detect any changes or missing devices.
- Change detection and notification: The system must send notifications to the admin in case of changes or missing devices.
- Device location module: The system should have a module to locate misplaced devices using Bluetooth or RFID technology.
- Location display: The system must show the current location of the misplaced device on the application interface.
- Video input processing: The system should be able to process and analyze video input to extract device information.
- Algorithm integration: The system must integrate the device identification data with the algorithm to determine if any issues have occurred.
- Admin communication: The system should provide a user-friendly interface for the admin to manage and monitor devices and receive notifications.

Non-functional requirements

The system should have a high level of accuracy in identifying the devices and their locations, and it should be able to detect any changes or missing items in a timely way. The system should also be able to identify misplaced devices utilizing Bluetooth or RFID technologies and display their present location to the admin through the application interface.

User requirements

- **Accurate device identification:** The system should be able to recognize and differentiate between various devices present in the workstation accurately.
- **Real-time monitoring:** The system should provide continuous, real-time monitoring of the workstation to detect any changes in the arrangement or missing devices promptly.
- **User-friendly interface:** The application interface should be easy to navigate and understand, allowing the admin to view device status and location information effortlessly.
- **Customizable settings:** The system should allow the admin to customize settings, such as defining specific devices to monitor, setting up alerts, and adjusting the frequency of monitoring.
- **Reliable notifications:** The system should send timely and reliable notifications to the admin whenever a change in arrangement or a missing device is detected.
- **Device tracking:** The system's Bluetooth or RFID module should accurately locate and track misplaced devices within a specified range.
- **Security and privacy:** The system should ensure the security and privacy of the data collected.

BUDGETARY PLAN

Component	Estimated Cost (Rs.)
Travel expenses	4000/-
Deployment cost	3700/-
Domain (if needed)	8900/-
Miscellaneous expenses	3400/-
Hardware (circuit)	30000/-
Total Cost Estimated	50000/-

Table 3: Budget

COMMERCIALIZATION

Target Audience

The following can be identified as the Target Audiences of MisplaceX.

- Companies with critical office areas such as data centers and server rooms
- IT administrators and support staff responsible for managing and maintaining the devices in the critical areas.
- Security personnel responsible for monitoring and ensuring the safety of the critical areas.
- Managers and executives who want to ensure the efficient and effective management of their company's critical areas and assets.
- Researchers and developers interested in the application of computer vision, machine learning, and location tracking technologies in security and asset management.

MARKET SPACE

the potential market space for MisplaceX could include:

- Enterprises: This product could be useful for enterprises that have critical office areas such as data centres and server rooms. It could help them ensure that all devices are arranged properly and prevent any potential security or operational issues.
- Security companies: Security companies could use this product to offer their clients an additional layer of protection by monitoring their critical office areas.
- IT departments: IT departments within organizations could use this product to monitor and maintain the proper arrangement of devices in their critical office areas.
- Facilities management companies: Facilities management companies could use this product to ensure that devices in critical office areas are arranged properly and to detect any misplaced devices.
- Government agencies: Government agencies that deal with sensitive information and have critical office areas could benefit from this product to maintain security and operational efficiency.

REFERENCES


- [1] N. M. a. K.-H. Kim, "Location-aware Management of End-User Devices using Wi-Fi Signals," *Journal of Information Processing Systems*, 2019.
- [2] L. A. M. a. J. A. López-Salcedo, "Real-Time Tracking and Localization of Multiple Devices in Indoor Environments Using Ultra-Wideband Technology," *Journal of Sensors*, 2019.
- [3] K. S. a. R. Kavitha, "Smart Location Tracking System for Large-scale Indoor Events using BLE Beacons," *Journal of Innovative Technology and Exploring Engineering*, 2019.
- [4] F.-Y. S. a. Y.-C. Chang, "A ZigBee-based positioning system for locating misplaced objects in an indoor environment," *Journal of Network and Computer Applications*, 2011.
- [5] W. Z. a. L. C. H. Chen, "A Bluetooth-based approach for locating misplaced objects in indoor environments," *Ambient Intelligence and Humanized Computing*, 2015.
- [6] Y. D. a. Y. Z. C. Zhang, "A UWB-based wireless sensor network for locating misplaced objects in indoor environments," *Journal of Sensors*, 2016.
- [7] S. L. a. X. L. Y. Chen, "An indoor localization and tracking system based on ultra-wideband technology," *Journal of Distributed Sensor Networks*, 2019.

APPENDIX

Similarity Report

It20028046 Gunathilaka S.B.M.B.S.A | Research proposal report IT20028046

?

**SLIIT**
Discover Your Future

Sri Lanka Institute of Information Technology

MisplaceX-IT device detection and monitoring system in office environments

Project proposal report

Project ID: 23-345

S.B.M.B.S.A Gunathilaka

Match Overview

2%

1

Submitted to Sri Lanka ...
Student Paper

1% >

2

Submitted to University...
Student Paper

<1% >

3

www.onepetro.org
Internet Source

<1% >

4

Submitted to Cerritos C...
Student Paper

<1% >

5

Submitted to CSU, San ...
Student Paper

<1% >

Figure 5:Turnitin similarity report