THE KNOWLEDGE UNIVERSITY

IT4010 – Research Project - 2023

Topic Assessment Form

Project ID : TMP-23-345

1. Topic (12 words max)

IT device detection and monitoring system in office environments

2. Research group the project belongs to

Machine Learning and Soft Computing (MLSC)

3. Research area the project belongs to

Image Processing (IP)

4. If a continuation of a previous project:

Project ID	
Year	

5. Team member details

Student Name	Student ID	Specialization
Leader: Herath H.M.C.S.B	IT19108100	CS
Member 2: Jasin Arachchi K.T.	IT20110802	CS
Member 3: Gunathilaka S.B.M.B.S.A	IT20028046	CS
Member 4: Jathurshan S	IT19130408	CSN

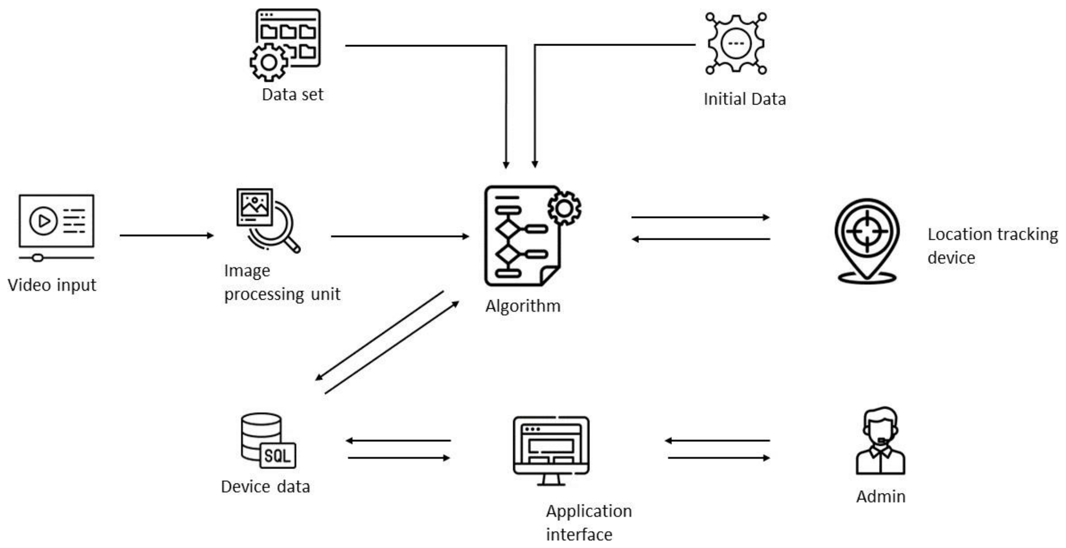
6. Brief description of the research problem including references (200 – 500 words max) – references not included in word count

Other than access control systems, it is rare to find a practical usage of image processing in office environments. Especially in the covid situation, some research is done to detect all the employees are wearing masks and managing their workspace while keeping their distance from others. But there is no research to protect IoT assets in an office environment using image processing. There can be misplacing of IoT assets or theft by an internal or external party. Even though the misplaced IT asset is on the premises, sometimes employees are unable to find it, mainly in data centers and server rooms, because there is so much equipment there. Especially in IT departments, employees deal with many assets within their working hours, so sometimes they forget where they put a particular asset. We can clearly see an unsolved problem with IT assets availability and their security in those places.

References

- Heidari, F. (2018, August 16). Munin: Study of area use and floor space occupation in office buildings using ML approach. In Munin: Study of area use and floor space occupation in office buildings using ML approach. https://munin.uit.no/handle/10037/15975
- A Surveillance System Controlling Covid-19 in Office Environments. (n.d.). In A Surveillance System Controlling Covid-19 in Office Environments | IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/10025286
- Yoo, S., Kim, S., Kim, E., Jung, E., Lee, K. H., & Hwang, H. (2018, September 10). Real-time location system-based asset tracking in the healthcare field: lessons learned from a feasibility study - BMC Medical Informatics and Decision Making. In BioMed Central. https://doi.org/10.1186/s12911-018-0656-0

7. Brief description of the nature of the solution including a conceptual diagram (250 words max)



First, the system requires video footage of a workstation. Here, we define a workstation as a working table with the necessary components like pc, laptops, routers, mouse, keyboards, etc. And there should be a user that has been assigned to that computer by a particular organization. Then this video footage will be forwarded to the image processing unit, giving the devices the necessary properties to identify exactly what that device is. Those details then provide to the algorithm, requiring the datasets and the initial data. Initial data means we give some information like these devices and components should be on the table for this particular workstation. Most of the time, it needs some data from the device data to verify the device. This database contains all allowed and denied devices according to the device policies, features, and capabilities. The algorithm will use those details when it verifies the detected devices from the video footage. If the system identifies a misplaced device, it instructs the location-tracking hardware component. This hardware component will be powered by an Arduino or raspberry pi board with some necessary modules that can interact with other technologies like Bluetooth, RFID, or GPS. A device or tracking tag will be attached internally or externally to the IT devices. The way those devices get power will be by a battery. We will create an application to interact with the device data database .this application is capable of viewing data in the database and editing those data, whitelisting or blacklisting device, and viewing the system outputs such as alerts. The application can also interact with the hardware component to track lost devices.

8. Brief description of specialized domain expertise, knowledge, and data requirements (300 words max)

Image Processing: Understanding of image processing techniques, such as object detection and tracking, image segmentation, and feature extraction is important for developing a system that can accurately detect and track devices in an office environment.

Computer Vision: Knowledge of computer vision algorithms and techniques, such as deep learning-based object detection and tracking, is essential for developing a system that can accurately detect and track devices in real-time.

IoT and Networking: Understanding of IoT and networking technologies, such as device communication protocols and cloud computing, is necessary for developing a system that can integrate with other IoT devices and systems in a smart office environment.

Machine Learning: Knowledge of machine learning algorithms and techniques, such as deep learning and convolutional neural networks, is important for developing a system that can learn from data and improve its accuracy over time.

Hence we are focusing on critical workstations such as workstations in a data centre, which is important to Understanding of that area including lighting conditions, device placement, and environment layouts are necessary for developing a system that can accurately detect and track devices in real-world conditions.

Data requirements for IoT device detection using image processing include high-quality images or video of the office environment, annotated data for training machine learning algorithms, and labeled data to evaluate the performance of the system. Access to large amounts of data is important for developing a system that can accurately detect and track devices in real-world conditions. To do this, we need enough datasets .some of them are given below for reference.

https://cocodataset.org/#explore?id=2389

https://data.world/us-nasa-gov/1013dee1-e4fa-4299-af63-ea7ae7651bf6

https://data.europa.eu/data/datasets/surs2983608s?locale=en

9. Objectives and Novelty

<table>
<tr><td colspan="4">Main Objective
develop a system that can accurately detect and track devices in an office environment. The system should be able to identify the arrangement of devices and detect if a device is missing from its intended place. The system should also be able to integrate with other IoT devices and systems in the office environment, providing real-time monitoring and tracking capabilities. The ultimate goal of the research is to provide a solution that can improve efficiency and productivity in the office by automating device tracking and management.</td></tr>
<tr><td>Member Name</td><td>Sub Objective</td><td>Tasks</td><td>Novelty</td></tr>
<tr><td>Jathurshan S</td><td>implement a real-time monitoring system for devices in an office environment that gives alerts for unauthorized or missing devices.</td><td>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</td><td>implement object detection algorithms using computer vision techniques to accurately identify and classify devices within the office environment.

Develop an algorithm to track the movement of devices within the office environment and identify when a device has been misplaced or removed.

Incorporate object recognition algorithms to</td></tr>
</table>

		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.	identify and categorize devices. This can improve the accuracy of the device monitoring and reduce false alarms. Automating the process of alerting the system admin when a device is missing or misplaced, instead of relying on manual reporting.
Herath H.M.C.S.B	creating a whitelist of authorized devices. This interface would allow the system admin to add or remove devices from the list, ensuring that only approved devices are allowed in the office area.	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.	Customizable permissions: Allow users to set custom permissions or restrictions for each device, providing more granular control over device access. Advanced access control: Implement advanced access control features,

		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: since we are using a combination of sensor inputs to have an accurate output, it is necessary to integrate this with the hardware component we build to locate misplaced devices and all other components. 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.	such as the ability to grant or deny access to specific functions or features of a device. Real-time reporting: Provide real-time reporting and notifications on device access attempts, including notifications sent to SIEM servers. Customizable alerts: Allow users to customize alerts, for example, to be notified when a device is blocked or when a device access attempt is made. Integration with other systems: Integrate this module with other systems, such as asset management or security information and event management (SIEM) systems, to provide a more complete solution.

		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. 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.	Real-time device management: Provide real-time device management capabilities, allowing users to manage their devices in near-real-time. User-friendly interface: Design a user-friendly interface that is intuitive and easy to use, making it accessible for users of all technical skill levels. Integration with other systems: Integrate this component with other systems, such as asset management systems, to provide a more complete solution. Automated device matching: Automate the process of matching device capabilities to organizational policies,

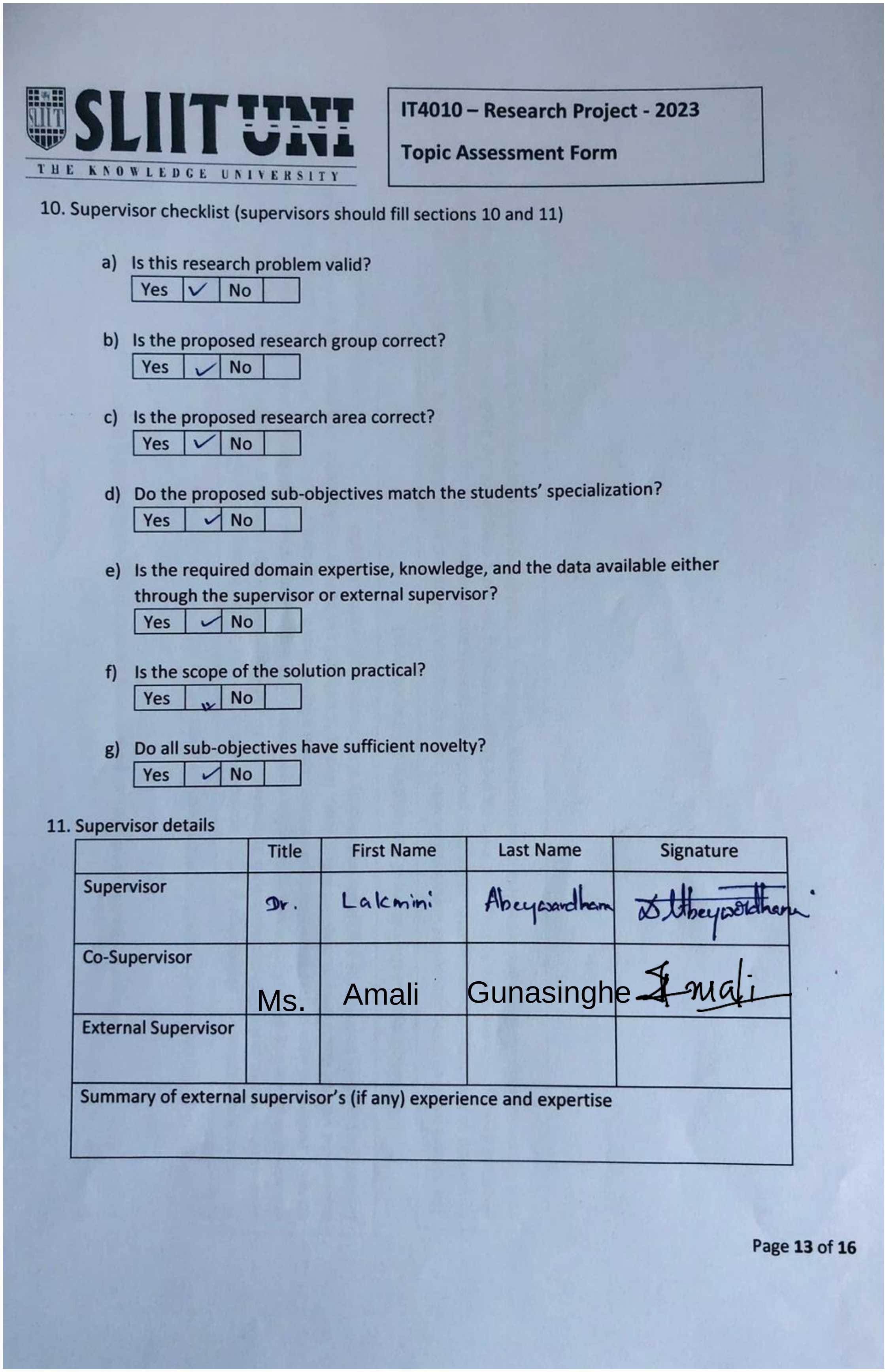
		Documentation: Document the design and implementation of the component to ensure that other team members and future developers can understand and maintain the system.	reducing the workload on system administrators. Personalized device access: Allow users to personalize their device access, for example, by setting up custom alerts or notifications. Efficient device management: Optimize the process of device management to ensure that it is efficient and requires minimal manual intervention.
Gunathilaka S.B.M.B.S.A	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,	Enhanced accuracy: improve the accuracy of the location tracking algorithms, for example, by using more advanced sensors or combining data from multiple sources. Real-time tracking: add real-time tracking capabilities to your module, allowing you to

		processing and analyzing 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,	see the current location of devices in near-real-time, rather than having to wait for updates. Indoor mapping: create an indoor map of the office environment, allowing you to easily visualize the location of devices and see where they are relative to each other. Integration with other systems: integrate this module with other systems, such as asset management systems, to provide a more complete solution. Customizable alerts: allow users to customize alerts, for example, to be notified when a device is moved out of a certain area or when a device is not in the right place.

		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.	Cost-effective: design a cost-effective solution that uses low-cost hardware components and efficient algorithms to reduce the overall cost of the system. Energy efficiency: focus on energy efficiency, for example, by using low-power sensors or optimizing the power usage of the microcontroller board.
Jasin Arachchi K.T.	Check user availability in critical workstation 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	Real-time monitoring: Implement real-time monitoring capabilities to provide real-time notifications and alerts when a vulnerability is detected. Predictive analytics: Use predictive analytics to identify potential vulnerabilities before they occur, allowing the security operations center

		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 an unusual activity is detected by the security operation center, 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, analyzing network traffic, and using other techniques to gather data. Integration with security operations center: Integrate the system with the security operation center, so that alerts and notifications can be sent to the appropriate personnel.	to proactively address them. User-friendly interface: Develop a user-friendly interface that allows security personnel to easily access and review the data and logs related to a particular vulnerability. Automated response: Develop an automated response system that can take action in response to a detected vulnerability, such as locking the device, shutting it down, or sending an alert to the security operations center. Integration with other systems: Integrate the system with other security and IT systems, such as intrusion detection systems, to provide a more

		Reporting: Develop a reporting mechanism to provide relevant information and data to the security operations center, including logs, activity metrics, and other relevant data.	comprehensive security solution.



SLIIT UNI
THE KNOWLEDGE UNIVERSITY

IT4010 – Research Project - 2023

Topic Assessment Form

10. Supervisor checklist (supervisors should fill sections 10 and 11)

a) Is this research problem valid?

Yes ☑ No □

b) Is the proposed research group correct?

Yes ☑ No □

c) Is the proposed research area correct?

Yes ☑ No □

d) Do the proposed sub-objectives match the students' specialization?

Yes ☑ No □

e) Is the required domain expertise, knowledge, and the data available either through the supervisor or external supervisor?

Yes ☑ No □

f) Is the scope of the solution practical?

Yes ☑ No □

g) Do all sub-objectives have sufficient novelty?

Yes ☑ No □

11. Supervisor details

	Title	First Name	Last Name	Signature
Supervisor	Dr.	Lakmini	Abeywardhana	Abeywardhana
Co-Supervisor	Ms.	Amali	Gunasinghe	Amali
External Supervisor				
Summary of external supervisor's (if any) experience and expertise				

IT4010 – Research Project - 2023

Topic Assessment Form

Summary Sheet

The topic evaluation panel will use the summary sheet to evaluate the suitability of the project

1. Brief description of research problem including references (200 – 300 words max)

The use of image processing technology in office environments is typically limited to access control systems and monitoring of employees' adherence to health and safety protocols such as wearing masks and maintaining social distancing. However, there is a potential for image processing to be used to protect IoT assets in the office environment. This is due to the issue of misplaced or stolen IoT assets, which can be a common problem in data centers and server rooms where there is a high density of equipment. IT departments, in particular, can struggle to keep track of the various assets they manage on a daily basis, leading to difficulties in locating missing items. As a result, there is a clear need for a solution that can help improve the availability and security of IoT assets in office environments.

2. Brief description of the nature of the solution (150 words max)

The system requires video footage of a workstation with the necessary components and a user assigned to it. This video footage is forwarded to the image processing unit, which then provides the datasets and initial data to the algorithm. The algorithm then verifies the detected devices from the video footage and instructs the location-tracking hardware component. An application is created to interact with the device data database and view data in the database, whitelisting or blacklisting device, and tracking lost devices.

3. Objectives and novelty

Main Objective This research aims to design a system that accurately detects and tracks devices in an office setting, integrating with other IoT devices and systems to improve efficiency and productivity.			
Member Name	Sub Objective	Tasks	Novelty
Jathurshan S	Monitoring devices in an office environment to detect unauthorized or missing devices.	The process involves installing and setting up image processing software or libraries, capturing images or video of the office environment, implementing algorithms for detecting and recognizing devices, storing information about authorized devices in a database, creating rules for device monitoring, implementing an alert system for notifications, and testing and fine-tuning the algorithms to ensure accuracy.	computer vision techniques to implement object detection and recognition algorithms for accurately identifying, categorizing, and tracking devices in an office environment. The system includes tracking the movement of devices, reducing false alarms through object recognition, and automating the process of alerting the system admin when a device is missing or misplaced.
Herath H.M.C.S.B	Create an interface and process the data	the development of a device management system for an office environment. This system includes the creation of whitelists and blacklists to authorize and restrict access to devices, access control based on the whitelist, integration with other components such as real-	the development of advanced device management capabilities for an office environment. The system includes customizable permissions and advanced access control, real-time reporting and notifications, customizable alerts, integration with other systems such as asset

		time monitoring and security, logging and reporting on device access attempts, device matching with organization policies, user interface development, testing and validation, and documentation.	management and SIEM, real-time device management, a user-friendly interface, automated device matching, personalized device access, and an efficient device management process.
Gunathilaka S.B.M.B.S.A	Build a module that can locate misplaced devices.	The tasks involves setting up the appropriate hardware components for tracking devices within an office environment, including microcontroller boards, sensors, and communication devices. The software development includes writing code to control the hardware components and integrate with other parts of the system. The location tracking involves developing algorithms to accurately track device locations. Testing and validation are crucial to ensure the module works accurately and integrates seamlessly with the rest of the system. Ongoing maintenance and support are also necessary to address any issues that arise in production and ensure the system continues to operate	the design and development of a device location tracking module for an office environment. The module will include hardware components such as a microcontroller board, sensors, and communication devices, as well as software code to control these components. The module will track the location of devices within the office environment using techniques such as triangulation, RFID, or BT signal strength. The module will be integrated with the rest of the system, including real-time monitoring and alerting, device access management, and security. The module will be tested, validated, and documented to ensure its accuracy, reliability, and maintainability. Ongoing support

		effectively. Documentation is important to understand and maintain the system by other team members and future developers.	and maintenance will also be provided. The focus will be on improving accuracy, providing real-time tracking, creating an indoor map, integrating with other systems, allowing for customizable alerts, being cost-effective, and being energy efficient.
Jasin Arachchi K.T.	Check user availability in critical workstation and generate alerts according to response and Bluetooth tracking.	The implementation of a device security system for an office environment includes user activity monitoring, vulnerability detection, unusual activity investigation, integration with the security operation center, and reporting. The system tracks user activity, detects security vulnerabilities, investigates unusual activity, and provides relevant information to the security operations center, which can then send alerts and notifications. The system also provides reporting capabilities to the security operations center, including logs, activity metrics, and other relevant data.	The system should provide real-time monitoring and use predictive analytics to identify potential vulnerabilities. The system should have a user-friendly interface and an automated response capability. The system should also be integrated with other security and IT systems to provide a comprehensive security solution.

SLIIT UNI
THE KNOWLEDGE UNIVERSITY

IT4010 – Research Project - 2023

Topic Assessment Form

<u>This part to be filled by the Topic Screening Panel members</u>

Acceptable: Mark/Select as necessary

Topic Assessment Accepted	
Topic Assessment Accepted with minor changes (should be followed up by the supervisor)*	
Topic Assessment to be Resubmitted with major changes*	
Topic Assessment Rejected. Topic must be changed	

* Detailed comments given below

Comments

The Review Panel Details

Member's Name	**Signature**

Important:

1. According to the comments given by the panel, do the necessary modifications and get the approval by the **Supervisor** or the **Same Panel**.
2. If the project topic is rejected, identify a new topic, and request the RP Team for a new topic assessment.
3. The form approved by the panel must be attached to the **Project Charter Form**.