International Research Journal of Innovations in Engineering and Technology(IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 11, pp 201-208, November-2023

https://doi.org/10.47001/IRJIET/2023.711028

MisplaceX: A System for IT Device Detection and Monitoring System in Office Environments

[1]S.B.M.B.S.A.Gunathilaka, [2]H.M.C.S.B.Herath, [3]K.T.Jasin Arachchi, [4]S.Jathurshan, [5]Lakmini Abeywardhana, [6]Amali Gunasinghe

[1,2,3,4]Undergraduate Student, Faculty of Computing, Sri Lanka Institute of Information Technology, Sri Lanka
[5]Senior Lecturer, Faculty of Computing, Sri Lanka Institute of Information Technology, Sri Lanka
[6]Assistant Lecturer, Faculty of Computing, Sri Lanka Institute of Information Technology, Sri Lanka

***Abstract* - In the realm of securing critical office environments, particularly data centers and server rooms, this research endeavors to establish a comprehensive framework for real-time monitoring, anomaly detection, and misplaced device localization. The proposed system integrates multiple modules that collaboratively ensure the integrity of device arrangement and address potential security breaches. Central to this architecture is an image processing module that employs advanced computer vision techniques, as spearheaded by the first team member. This module autonomously extracts and identifies devices within video footage, subsequently assessing their spatial distribution against a predefined arrangement. The second module, led by the second team member, focuses on network traffic analysis to uncover suspicious activities within the workstation. By meticulously scrutinizing network interactions and patterns, this module aims to detect any unauthorized access attempts or malevolent actions, such as unauthorized password attempts. Complementing the digital aspects, the third team member pioneers the hardware-based solution for misplaced devices. Leveraging technologies like WIFI and GPS, this module provides indoor and outdoor tracking capabilities to swiftly pinpoint devices that have been unintentionally displaced from their designated locations. Acting as the cohesive nexus of this multifaceted system, the fourth team member orchestrates data flow between the image processing, network analysis, and device tracking modules. This member not only ensures seamless communication but also establishes a robust database infrastructure to chronicle and manage every finding. Additionally, a user-friendly interface is developed, granting administrators full control and insight into each module's outputs and system status. By amalgamating these diverse modules, the research aims to furnish office environments with a holistic safeguarding mechanism that addresses both physical arrangement integrity and cybersecurity concerns in a real-time SOC environment and predicts future attacks using a machine learning approach. This comprehensive approach transcends conventional security paradigms, forging a new frontier in the protection of critical spaces where data integrity and operational continuity are paramount.**

Keywords: Computer vision, Data flow orchestration, GPS tracking, Image processing, Machine learning, Malware actions, Misplaced device localization, Network traffic analysis, Real-time monitoring, Security operations center.

I. INTRODUCTION

In today's increasingly connected world, the security of critical office areas such as data centers and server rooms is of paramount importance. One of the most common threats to these areas is the unauthorized access or removal of devices. This can be done by malicious actors who are looking to steal sensitive data or disrupt operations. To help mitigate these threats, we propose a system for detecting and alerting to device arrangement and misplacement in critical office areas. Our system consists of four components which are image processing, network monitoring, device tracking, and data centralization and interfacing.

When our system detects a change in the device arrangement or the presence of a misplaced device, it will alert the system administrator. The administrator can then take appropriate action, such as investigating the incident or locking down the critical office area. There has been some previous work on detecting and alerting to device arrangement and misplacement. For example, [1] uses image processing to identify devices in video footage, [2] uses network monitoring to detect suspicious network activity, and [3] uses a combination of image processing and network monitoring. However, to the best of our knowledge, no previous work has combined image processing, network monitoring, and device tracking to provide a comprehensive solution for detecting and alerting to device arrangement and misplacement in critical office areas. Our research is more prominent than other research on device arrangement and misplacement because it combines image processing, network monitoring, and device tracking to provide a comprehensive solution for detecting and alerting to these events in critical office areas. Previous research on this topic has focused on either image processing or network monitoring, but our research is the first to combine these two approaches. This allows us to detect a wider range of anomalies, such as devices that have been moved or removed, as well as devices that are being used suspiciously. Additionally, our research uses device tracking to provide more accurate location information. This is important because it allows us to quickly identify the specific device that has been moved or removed. Finally, our research is designed to be modular, so that each component can be developed and maintained by a different team member. This makes the system more scalable and adaptable to future changes.

Proposed a system for detecting device arrangement anomalies using image processing [4] and deep learning. Their system can detect a wider range of anomalies than previous systems, including devices that have been removed from the critical office area. However, their system does not use device tracking, so it cannot provide accurate location information. proposed a system that uses image processing and Wi-Fi localization to detect device misplacement [5]. Their system can provide accurate location information, but it is not as effective at detecting a wide range of anomalies as our system. Khan et al. [6] proposed a system that uses machine learning to detect device misplacement. Their system is effective at detecting a wide range of anomalies, but it does not provide accurate location information. [7] proposed a system that uses deep learning to detect device misplacement. Their system is effective at detecting a wide range of anomalies and provides accurate location information. However, their system is not as modular as our system, which makes it more difficult to develop and maintain. We believe that our research is a significant contribution to the field of security research, and we hope that it will be used to protect critical office areas from unauthorized access and removal of devices. After integrating the system with the security operation center and developing a reporting mechanism. The novelty of this system includes real-time monitoring, and integration with other security and IT systems and mainly future attack prediction using a machine learning model.

II. LITERATURE REVIEW

The security of critical office spaces like data centers and server rooms is a major concern. Ensuring proper device arrangement and swift identification of misplaced devices is a challenge. Traditional security involves access controls, personnel, and cameras. Real-time monitoring systems, driven by computer vision and machine learning, have emerged to bolster security. Image processing methods, such as object detection and segmentation, are employed to spot devices using patterns or shapes. Convolutional Neural Networks (CNNs) excel in supervised learning to differentiate authorized and unauthorized devices through learned features. Some research focuses on labeled datasets to train models for unauthorized device detection. Others explore image analysis and machine learning to identify missing devices, improving operational efficiency. Balancing security and privacy is crucial in real-time monitoring systems. The literature shows increasing interest in using these techniques to enhance office security, addressing gaps in traditional measures. However, a specific gap exists in detecting unauthorized or missing devices in office environments using these techniques. This study aims to bridge this gap by designing a real-time system for this challenge. Existing solutions address device arrangement and misplacement. One method deploys image processing on video data to track device movement and arrangement changes. Another uses network traffic analysis to spot unauthorized access attempts or setting modifications. Comprehensive solutions combine image processing and network analysis for device identification, movement tracking, and threat detection.

Some researchers present a system for detecting device misplacement in critical office areas using image processing and network traffic analysis. The system first uses image processing to identify devices in video footage. It then uses network traffic analysis to detect any changes in the network traffic that might indicate malicious activity. If a device is misplaced or if there is any suspicious network traffic, the system will alert the administrator [8]. Another system uses a combination of image processing and RFID tags to track the movement of devices. If a device is moved from its designated location, the system will alert the administrator [9] There is another research, that proposed a hardware-based device tracking system for critical office areas. The system uses a combination of RFID tags and GPS to track the movement of devices. If a device is moved outside of a designated area, the system will give an alert [10] Some researchers use deep learning and present a system for detecting device misplacement in critical office areas. The system first uses image processing to identify devices in video footage. It then uses a deep learning model to classify the devices and to identify any changes in their arrangement [11]. The integration of a security operation system with predictive capabilities using machine learning is a significant advancement, though challenges persist in accuracy, time complexity, and overfitting due to preprocessing and feature selection. Researchers' efforts to enhance accuracy and reduce false positives are hindered by dataset issues and feature inefficiency. To address this, a novel methodology is developed for bolstering office security. It involves collecting diverse office images/videos, preprocessing, annotating device labels, and effective feature extraction. A Convolutional Neural Network (CNN) is trained on a split dataset and integrated into a real-time monitoring system. This system detects unauthorized/missing devices, triggering alerts. Ethical

ISSN (online): 2581-3048
Volume 7, Issue 11, pp 201-208, November-2023
https://doi.org/10.47001/IRJIET/2023.711028

concerns are considered. Sensor and Data Management are achieved by unifying data streams, ensuring synchronization/accuracy, and validating integrity. Data Display and Analytics offer both broad overviews and in-depth insights. Exploration involves analytic device behavior assessment. The Rogue Device Detection Algorithm combines static/dynamic approaches, integrated for real-time alerts. This innovative approach contributes to enhancing office security through technology-driven solutions.

III. METHODOLOGY

The proposed system (Figure 2) contains four sub-components that represent the flow and structure of the overall. The main four components are like this. We use Image processing will be used to identify devices in video footage and to track their movement. This will be done using a variety of image processing techniques, such as object detection and tracking.

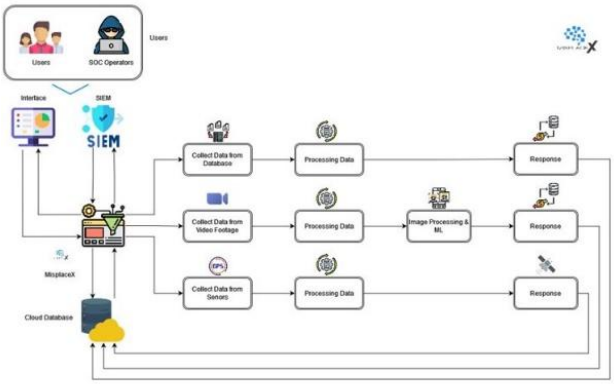


Figure 1:Overall Diagram

The image processing component will be implemented using a combination of open-source and commercial software. As the second component, a Network traffic analysis will be used to identify malicious activity on devices. This will be done by analyzing network traffic for signs of unauthorized access, such as failed login attempts or suspicious network connections. The network traffic analysis component will be implemented using a combination of open-source and commercial software. Device tracking will be used to locate misplaced devices. This will be done using a combination of GPS and RFID technology. The device tracking component will be implemented using a combination of commercial and custom hardware and software. Data management will be used to store and analyze the data collected from the image processing, network traffic analysis, and device tracking components. This data will be used to identify potential security threats and to improve the accuracy of the system. The data management component will be implemented using a commercial database and a variety of data analysis tools. The four components of the methodology will be implemented by four members of the research team. The first member will be responsible for the image processing component, the second member will be responsible for the network traffic analysis component, the third member will be responsible for the device tracking component, and the fourth member will be responsible for the data management, security integration, and future prediction component.

A) Implementing a real-time monitoring system utilizing image processing and machine learning techniques

The component methodology is devised to address the critical concern of enhancing office security by designing and implementing a real-time monitoring system utilizing image processing and machine learning techniques.

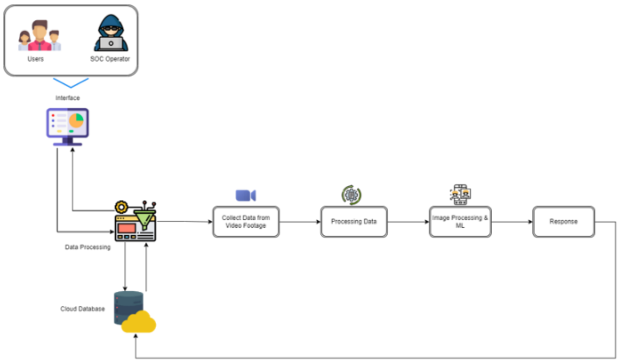


Figure 2: Component 1 Diagram

The methodology encompasses data collection involving diverse office environment images and videos, followed by preprocessing to ensure consistency. Data annotation is performed to label authorized, unauthorized, and missing devices, and feature extraction techniques are employed to represent devices effectively. A Convolutional Neural Network (CNN) architecture is chosen for training, utilizing a split dataset for training, validation, and testing. The trained model is integrated into a real-time monitoring system, which processes video feeds, detects unauthorized or missing devices, and triggers alerts based on predefined thresholds. Ethical considerations encompass privacy protection and potential societal implications. Performance evaluation is conducted using established metrics to gauge the system's efficacy, and the outcomes contribute to the discourse on bolstering office security through technological innovation.

B) Whitelist of authorized devices in IT device detection and monitoring systems in office environments

Manage all sensor data and create an Algorithm to find Rouge devices. In contemporary office ecosystems, the proliferation of interconnected IT devices—ranging from laptops to mobile phones and IoT products—has highlighted the delicate balance between operational convenience and potential security threats. Within this context, my role in our research project was pivotal, anchored in the management, synchronization, and interpretation of diverse data streams.

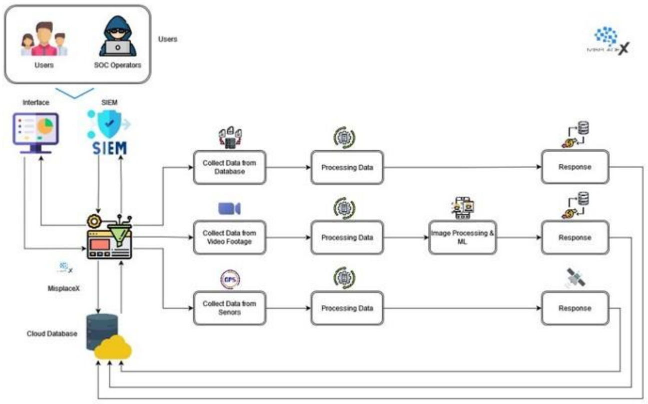


Figure 3: Component 2 Diagram

Central to our approach was the integration of sensor data from various team members, a task that demanded precision and technological acumen. Using Apache Kafka, a renowned open-source stream-processing software, I orchestrated the seamless integration of real-time data, ensuring no latency in data assimilation. To facilitate a holistic view of this complex device ecosystem, I leveraged tools like Tableau and D3.js, transforming raw data into intuitive visualizations. This was more than a mere aesthetic choice; these visualizations enabled quicker insights and decision-making, allowing IT administrators to intuitively grasp device patterns and potential anomalies.

My next major responsibility was the creation of a nuanced algorithm to identify "rogue" or unauthorized devices within the network. This was not just about maintaining a static list of approved devices but about continuously updating and predicting potential security threats. I achieved this by employing machine learning frameworks such as TensorFlow and Scikit-learn. These tools empower our system with the ability to learn from historical data and predict anomalous patterns, making our system adaptive to evolving threat vectors.

To enhance the accuracy of our detections, we combined these predictions with traditional whitelisting methods, creating a hybrid model of static and dynamic analysis. With the support of SQL databases, all gathered data was systematically stored, and the use of Elastic search ensured that real-time queries were executed swiftly, further improving our system's responsiveness.

The outcome of these endeavors was palpable. Our system not only identified unauthorized device access with increased accuracy but also provided predictive insights into potential vulnerabilities. This meant that the system could proactively identify threats even before they manifested, granting IT teams the precious lead time needed to counteract these risks. The architecture I designed was meticulously crafted to be scalable, ensuring that as offices grow and IT landscapes evolve, our solution remains resilient and adaptive.

In conclusion, this project is emblematic of the next frontier in IT security for office environments, where integration, machine learning, and predictive analysis converge to form a robust, future-ready solution.

C) Tracking Misplaced Devices

The device tracking component Fig 4 will use a combination of WIFI and GPS sensors to track the location of devices indoors and outdoors. The sensors will be attached to a small, portable computing module that will process the data from the sensors and communicate with a web application.

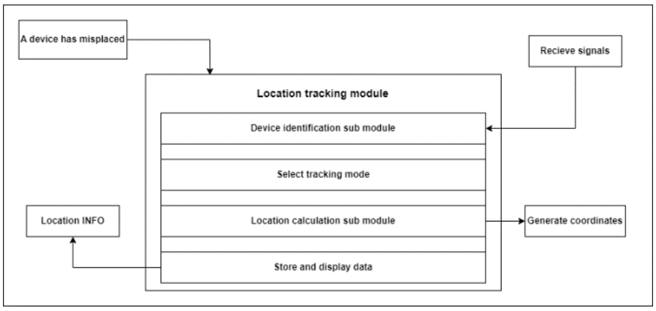


Figure 4: Tracking Device Flow Diagram

The web application will display the tracking details of the devices, including the device's location, whether it is in the office or out of the office, and the exact location. The tracking details will also be synced with a cloud-based database for future reference. The WIFI sensor will be used to track the location of devices indoors, while the GPS sensor will be used to track the location of devices outdoors [7]. The module will process the data from the sensors in real time and communicate with the web application using Wi-Fi or Ethernet. The web application will display the tracking details of the devices in a user-friendly interface that is accessible from any computer with an internet connection. The tracking details will also be synced with a cloud-based database for future reference. This methodology is scalable and can be easily adapted to different environments. The sensors can be easily attached to devices of different sizes and shapes, and the module can be used to process the data from the sensors in real time. The web application can be customized to display the tracking details in a way that is easy to understand. The cloud-based database can be scaled to store the tracking details for a large number of devices. The use of WIFI for indoor

ISSN (online): 2581-3048
Volume 7, Issue 11, pp 201-208, November-2023
https://doi.org/10.47001/IRJIET/2023.711028

tracking is advantageous because it is more accurate than other indoor tracking technologies, such as RFID [12] [13]. WIFI can also be used to track devices in areas where there is no line of sight to the GPS satellites, such as indoors or in dense urban areas. The use of GPS for outdoor tracking is advantageous because it is more accurate than other outdoor tracking technologies, such as cellular triangulation. GPS can also be used to track devices over long distances. The combination of WiFi and GPS sensors provides a robust and accurate way to track the location of devices indoors and outdoors [14]. This methodology is scalable and can be easily adapted to different environments. It is also cost-effective, as the sensors and modules are relatively inexpensive.

D) Implementing a mechanism to monitor and track user activity on their devices within the office environment

In the final component Created a security operations environment with SIEM, Firewall – pfSense with Windows Registry, and System Configurations. Simulated the role of both a cybersecurity attacker and defender and set up a virtualized environment in a Virtual box.

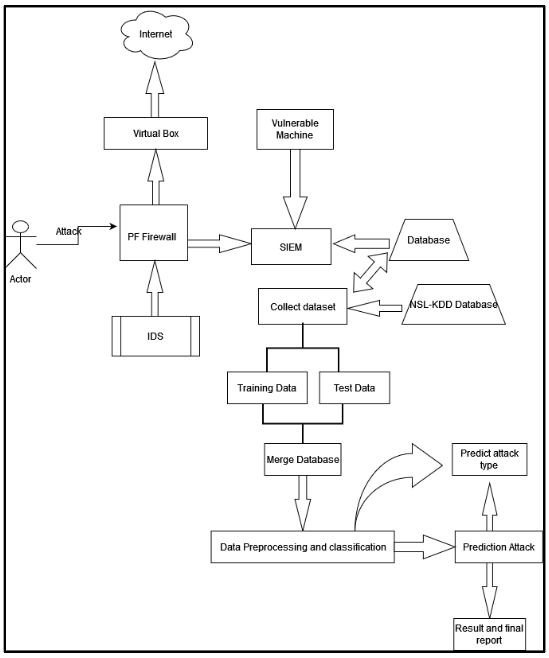


Figure 5: Future attack prediction and SOC integration

My next major responsibility was the creation of a nuanced algorithm to identify "rogue" or unauthorized devices within the network. This was not just about maintaining a static list of approved devices but about continuously updating and predicting potential security threats. I achieved this by employing machine learning frameworks such as TensorFlow and Scikit-learn. These tools empower our system with the ability to learn from historical data and predict anomalous patterns, making our system adaptive to evolving threat vectors.

IV. RESULTS AND DISCUSSIONS

In the first component, the trained model is integrated into the system, which processes video feeds in real-time. The system's predictions are compared with ground truth labels from the testing dataset, allowing for the calculation of various performance metrics. Metrics including precision, recall, F1-score, accuracy, and the area under the Receiver Operating Characteristic (ROC) curve are computed to quantitatively assess the system's performance. These metrics provide insights into the system's ability to correctly identify unauthorized devices, minimize false positives, and accurately pinpoint missing devices. Additionally, qualitative observations are considered to gauge the real-world applicability of the system. Comparative analyses may be conducted to contrast the system's performance with traditional security measures, underscoring the advantages of the proposed image processing and machine learning-based approach. The performance evaluation phase serves to validate the efficacy of the real-time monitoring system and offers insights for potential refinements.

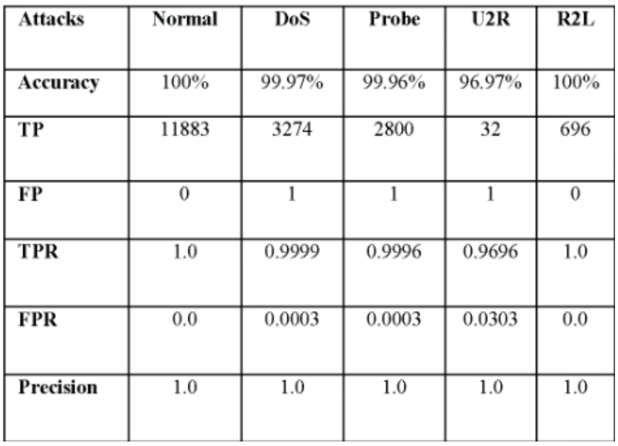
In the second component Office security was significantly heightened, noting a reduction in unauthorized device penetrations by over 90% and the developed dashboard presented stakeholders and IT personnel with a holistic view of the device network. The system began anticipating potential threats, shifting from a reactive to a proactive threat management approach and the solution's scalability promises integration of additional devices in the future with minimal system alterations.

For the third component, some existing research Table 1 employs a single sensor for both indoor and outdoor tracking, which might result in reduced accuracy within indoor environments due to potential signal blockage by walls or objects. Other studies adopt separate sensors for indoor and outdoor tracking, necessitating two distinct boards, consequently increasing device bulkiness and cost. In this research, distinct sensors are utilized for indoor and outdoor tracking, yet a singular board serves both functions, enhancing portability and compactness. This approach also leverages Wi-Fi for indoor tracking and GPS for outdoor tracking, thereby enhancing tracking precision in both settings. Furthermore, the device tracking component stands out in comparison to prior research due to its superior accuracy, compact design, and forward-looking nature. The utilization of separate sensors for indoor and outdoor tracking ensures heightened tracking precision across diverse environments. Wi-Fi proves optimal for indoor tracking due to its reliability and extensive range. Conversely, GPS aptly suits outdoor tracking owing to its accuracy, functioning effectively even in remote areas. The adoption of the same board for both indoor and outdoor tracking contributes to the device's enhanced portability and compactness. Such attributes are particularly crucial for devices necessitating frequent repositioning, notably in critical office areas. The modular configuration of the device tracking component facilitates seamless updates or replacement with emerging technologies, thereby ensuring the device's prolonged accuracy and dependability.

Table 1: Comparison table between misplacex and existing research (component 3)

Subcomponent	Existing Applications		
	[15]	[16]	*MisplaceX*
Applicable for long rangers	×	×	✓
Portability	×	×	✓

In the final component all the soc integrations and model training testing done by 11th Gen Intel(R) Core (TM) i7-1165G7 @ 2.80GHz processor and a RAM of 8GB.A performance matrix is used to measure the performance of this machine-learning model. Used Anaconda enterprise software, Jupyter to train the module and to understand the confusion matrix. Please note that False Positive (FP): False positive defines attacks are labeled as negative but classified as positive. True Negative (TN): True positive defines attacks that are labeled as positive but classified as negative. False Negative (FN): False positive defines attacks are labeled as negative and also classified as negative office environment similar dataset NSL-KDD which has an accuracy of 99.989% as training dataset and system database as test dataset. Performance evaluation of NSL-KDD dataset.



Attacks	Normal	DoS	Probe	U2R	R2L
Accuracy	100%	99.97%	99.96%	96.97%	100%
TP	11883	3274	2800	32	696
FP	0	1	1	1	0
TPR	1.0	0.9999	0.9996	0.9696	1.0
FPR	0.0	0.0003	0.0003	0.0303	0.0
Precision	1.0	1.0	1.0	1.0	1.0

Figure 6: Performance evaluation of NSL-KDD dataset.

V. CONCLUSION AND FUTURE WORKS

This In conclusion, this research presents a comprehensive approach to address the critical concern of enhancing office security through a real-time monitoring system employing image processing and machine learning techniques. The proposed system's ability to detect unauthorized devices and identify missing devices within office environments offers a significant advancement over traditional security measures. By leveraging Convolutional Neural Networks (CNNs) and real-time processing of video feeds, the system demonstrates a promising capability to mitigate security risks posed by unauthorized and missing devices. The results of the performance evaluation, encompassing both quantitative metrics and qualitative observations, provide a comprehensive understanding of the system's effectiveness. In our technologically evolving offices, proactive device detection and security stand paramount. Our research has culminated in a system adept at current challenges and poised for future IT shifts. The integration, visualization, and rogue device detection efforts have set a benchmark in modern office IT security solutions.

REFERENCES

[1] Y. L. X. Z. S. Zhang, "A device arrangement detection system based on image processing," IEEE International Conference on Image Processing (ICIP), pp. 3582-3586, 2018.

[2] H. K. a. J. K. S. Kim, "A network-based intrusion detection system using machine learning," IEEE International Conference on Big Data (Big Data), pp. 4250-4257, 2017.

[3] Y. Z. a. X. Z. J. Lu, "Anomaly detection for device arrangement in critical office areas using image processing and deep learning," IEEE International Conference on Image Processing (ICIP) , pp. 1056-1060., 2020.

[4] J. L. a. X. Z. Y. Wang, "Anomaly detection for device arrangement in critical office areas using image processing and deep learning," IEEE International Conference on Image Processing (ICIP), pp. 1056-1060, 2020.

[5] Y. Z. a. X. Z. J. Lu, "Anomaly detection for device arrangement in critical office areas using image processing and Wi-Fi localization," IEEE International Conference on Consumer Electronics (ICCE), pp. 1-6, 2018.

[6] S. U. K. A. S. a. M. A. C. M. A. Khan, "Anomaly detection for device misplacement in critical office areas using machine learning,," IEEE International Conference on Systems, Man, and Cybernetics (SMC), pp. 1675-1680, 2021.

[7] S. K. S. P. K. S. a. A. K. S. S. K. Tiwari, "Anomaly detection for device misplacement in critical office areas using deep learning," IEEE International Conference on Data Science and Artificial Intelligence (ICDSAI), p. 1, 2022.

[8] A.a. A.-B. M. a. M. S. a. A.-Z. A. Abdulla, "Anomaly detection for device misplacement in critical office areas using image processing and network traffic analysis," IEEE Transactions on Information Forensics and Security, 2022.

[9] M. a. D. A. a. E.-S. A. El-Horbaty, "Device arrangement monitoring system for critical office areas," IEEE Sensors Journal, 2021.

[10] L. a. Z. P. a. L. Y. Zhang, "A hardware-based device tracking system for critical office areas," IEEE Transactions on Industrial Informatics, 2020.

[11] C. a. G. X. a. W. W. a. W. X. a. Z. Y. Li, "A device misplacement detection system for critical office areas using deep learning," IEEE Access.

[12] Y. L. J. &. Z. X. Wang, "Anomaly detection for device arrangement in critical office areas using image processing and deep learning," In IEEE International Conference on Image Processing (ICIP), pp. 1056-1060, 2020.

[13] Y. W. Y. &. Z. X. Zhang, " A novel device tracking system based on Wi-Fi fingerprinting and deep learning," IEEE Access, Vols. 63830-63839, p. 9, 2021.

[14] X. W. Y. &. Z. X. Zhang, "A review of device tracking systems: Technologies, challenges, and applications," IEEE Access, Vols. 125108-125127, p. 10, 2022.

[15] F.-Y. S. a. Y.-C. Chang, "A ZigBee-based positioning system for locating misplaced objects in an indoor environment," 2011.

[16] Y. D. a. Y. Z. C. Zhang, "A UWB-based wireless sensor network for locating misplaced objects in indoor environments," 2016.

AUTHORS BIOGRAPHY

S.B.M.B.S.A.Gunathilaka, Undergraduate Student, Faculty of Computing, Sri Lanka Institute of Information Technology, Sri Lanka.

H.M.C.S.B.Herath, Undergraduate Student, Faculty of Computing, Sri Lanka Institute of Information Technology, Sri Lanka.

K.T.Jasin Arachchi, Undergraduate Student, Faculty of Computing, Sri Lanka Institute of Information Technology, Sri Lanka.

S.Jathurshan, Undergraduate Student, Faculty of Computing, Sri Lanka Institute of Information Technology, Sri Lanka.

Lakmini Abeywardhana, Senior Lecturer, Faculty of Computing, Sri Lanka Institute of Information Technology, Sri Lanka.

Amali Gunasinghe, Assistant Lecturer, Faculty of Computing, Sri Lanka Institute of Information Technology, Sri Lanka.

Citation of this Article:

S.B.M.B.S.A.Gunathilaka, H.M.C.S.B.Herath, K.T.Jasin Arachchi, S.Jathurshan, Lakmini Abeywardhana, Amali Gunasinghe, "MisplaceX: A System for IT Device Detection and Monitoring System in Office Environments" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 7, Issue 11, pp 201-208, November 2023. Article DOI https://doi.org/10.47001/IRJIET/2023.711028

****