International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 04 | April - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Enhancing Video Call Safety Without Alerting Recipients

Andey Alekhya
BTech Student, Dept. of CSE
Institute of Aeronautical Engineering
Hyderabad, India
21951A0506@iare.ac.in

Challuri Vedakshari
BTech Student, Dept. of CSE
Institute of Aeronautical Engineering
Hyderabad, India
22955A0524@iare.ac.in

Vakode Purushotham
BTech Student, Dept. of CSE
Institute of Aeronautical Engineering
Hyderabad, India
21951A05E2@iare.ac.in

Dr. D. Durga Bhavani
Associate Professor, Dept. of CSE
Institute of Aeronautical Engineering
Hyderabad, India
d.durgabhavani@iare.ac.in

***Abstract*—This project focuses on developing a real-time suspicious activity detection system using a pre-trained TensorFlow object detection model. The system integrates video analysis, audio processing, and email notification capabilities. It utilizes OpenCV for video stream processing and PyAudio for audio capture. A phone call simulation feature is embedded to trigger automated responses, simulating real-world security scenarios. The system is equipped with an email alert mechanism, sending notifications when certain predefined conditions are met. A graphical user interface (GUI) built with Tkinter enhances user interaction, providing an accessible and efficient tool for monitoring suspicious activities. This project showcases an advanced fusio of machine learning, computer vision, and real-time alert systems for enhanced security and monitoring applications.**

By leveraging real-time data processing and a simple GUI interface, this tool aids in proactive security measures and monitoring. This abstract captures the main functionalities, ensuring originality and clear articulation of the project's objectives.

Keywords: Suspicious Activity Detection, Machine Learning, Call Monitoring, Communication Security

I. INTRODUCTION

In recent years, the rise of advanced technologies in computer vision and artificial intelligence has revolutionized security and surveillance systems. Traditional surveillance setups, often reliant on manual observation, are limited by human fatigue and attention span. Automated systems, capable of real-time monitoring and rapid response, are becoming essential in various sectors.

This project presents a system for detecting suspicious activities by integrating image processing, machine learning, and audio analysis. The system leverages OpenCV for video capture and real-time processing, combined with a pre-trained TensorFlow model to recognize objects or behaviors that could indicate potential threats. In the event of detection, the system autonomously alerts designated personnel via email, using the Simple Mail Transfer Protocol (SMTP), ensuring timely response. With the increasing digitization of services and infrastructure, cybersecurity has become a paramount concern for organizations and individuals alike. The rapid expansion of online interactions has led to a corresponding rise in cyber threats, making the detection and prevention of suspicious activities. Despite advances in cybersecurity frameworks, many systems remain vulnerable to sophisticated attacks that often go undetected until after significant damage has been done. Traditional methods of identifying suspicious activity have proven insufficient due to their reliance on predefined patterns, which limits their effectiveness in dealing with emerging threats.

The primary objective of this work is to develop an enhanced detection system that leverages machine learning techniques to identify suspicious activities in real-time. Unlike conventional methods, our approach adapts to evolving threats by continuously learning from new data, offering a more responsive and accurate defense mechanism. Furthermore, the system incorporates audio capabilities to simulate phone call interactions, allowing for additional verification measures. A user-friendly graphical interface facilitates easy monitoring and control. By blending cutting-edge technologies with practical applications, this project aims to provide a scalable and effective solution for enhancing security and threat detection in various environments.

II. EASE OF USE

A. Maintaining the Integrity of the Specifications

The need for advanced security systems has led to the development of automated solutions that leverage cutting-edge technologies in image processing and machine learning. Traditional surveillance methods, dependent on manual observation, often suffer from inefficiency due to human limitations. In contrast, intelligent systems capable of real-time threat detection and automated response have become critical for ensuring security in modern environments. This project aims to create a comprehensive suspicious activity detection system by combining several technologies, including computer vision, machine learning, and audio analysis. The system captures video data using OpenCV and processes it using a pre-trained TensorFlow model to identify potentially suspicious objects or activities. Upon detection, the system immediately sends alerts to designated recipients via email using the Simple Mail Transfer Protocol (SMTP), ensuring a swift and automated response to potential threats.

By integrating these advanced features, this system offers a robust and scalable approach to threat detection, making it suitable for various environments such as homes, offices, and public spaces where security is of paramount importance. The combination of real-time video and audio analysis, along with prompt notification, ensures a proactive approach to security management.

III. EXISTING APPROACH

The detection of suspicious activity in communication systems and networks has been a topic of significant research. Traditionally, the following approaches have been employed to identify anomalies:

Early methods relied on predefined rules to detect anomalies or suspicious behavior. These systems were configured with specific thresholds, such as call duration limits or unusual communication frequencies. Although these systems are straightforward, they are often rigid and can generate a high rate of false positives or miss sophisticated attacks.

Signature-based systems look for known patterns of suspicious activity, such as specific attack signatures or well-documented fraud behaviors. While effective at catching known threats, they fail when novel or zero-day attacks occur since they rely on predefined patterns. In the absence of labeled datasets, unsupervised learning algorithms like **Isolation Forest** or **Autoencoders** are used to detect anomalies. These algorithms model what is considered "normal" behavior and flag activities that differ from the norm. Unsupervised approaches are more adaptable but may require fine-tuning to avoid false positives.

IV. PROBLEM STATEMENT

In an increasingly digital world, communication systems such as voice, video calls, and network communication channels are often vulnerable to misuse, fraud, and malicious activities. Current security measures often rely on rule-based or signature-based detection techniques that are insufficient to address evolving threats. These methods struggle with adaptability, generate high rates of false positives, and fail to detect sophisticated or novel suspicious activities.

Moreover, the vast volume of real-time communication data, varying user behavior patterns, and dynamic network conditions make it challenging to maintain accurate detection systems. This can result in undetected fraudulent activities, compromised user data, and significant security breaches.

Thus, there is a need for an intelligent, adaptable, and efficient system capable of detecting suspicious activities in real-time, while minimizing false positives and maintaining scalability for large-scale communications.

V. PROPOSED SYSTEM

The proposed system is a real-time suspicious activity detection framework that integrates multiple technologies to enhance security monitoring. It combines video surveillance, machine learning for object detection, and automated alert mechanisms, ensuring timely responses to potential threats. The system operates by capturing video feeds using OpenCV, an open-source computer vision library. The captured data is then processed by a pre-trained TensorFlow model, which is specifically designed to identify suspicious objects or behaviors. This model is capable of recognizing various patterns and anomalies in the video feed, allowing it to detect potential threats in real time.

Upon detecting suspicious activity, the system automatically generates an alert. This alert is sent via email using SMTP, enabling immediate notification of the relevant parties. The email system is integrated with a secure protocol to ensure reliable and prompt delivery of alerts, facilitating quick responses to security breaches or unusual activities. Additionally, the system simulates a phone call as a secondary verification measure. It rings a designated number and tracks whether the call is answered. If the call is not answered after a set number of rings, it is logged as unanswered, adding an additional layer of validation to the alerting process. This feature enhances the system's ability to confirm the severity of a detected threat. To simplify user interaction, a Graphical User Interface (GUI) is developed using Tkinter, providing users with easy access to controls and monitoring features. This interface allows users to configure settings, view the status of the system, and manage alerts, offering an intuitive way to oversee security operations.

In summary, the proposed system is a highly efficient and scalable security solution that integrates real-time video analysis, machine learning-driven detection, automated email alerts, and

simulated phone call verification. It is designed to be flexible and adaptable for use in diverse environments, including homes, offices, and public spaces, where rapid detection and response to suspicious activities are essential.

A. System Architecture

Fig:1 System Architecture

The architecture of the suspicious activity detection system is designed to integrate multiple components for real-time monitoring, detection, alerting, and user interaction. Each part of the system works together to ensure seamless detection of unusual activities and prompt notifications. Below is a breakdown of the architecture:

1. Video Capture (OpenCV):

The system starts by capturing video feeds from cameras using OpenCV, a popular library for computer vision tasks. This module continuously captures frames in real-time, serving as the input to the object detection model.

2. Object Detection (TensorFlow Model):

The captured video feed is processed by a pre-trained object detection model built with TensorFlow. The model analyzes each frame to identify suspicious objects or behaviors. It uses deep learning techniques to recognize patterns that may indicate potential threats or unusual activities.

3. Alert System (Email Notifications - SMTP):

Once a suspicious activity is detected by the TensorFlow model, an automated email alert is generated using the Simple Mail Transfer Protocol (SMTP). This ensures that designated individuals or authorities are immediately notified about the potential threat.

4. Simulated Phone Call Verification:

As an additional verification step, the system simulates a phone call to a pre-configured number. This functionality helps to ensure that alerts are followed up in real time. If the call is unanswered, it is logged, providing further validation of the detection.

5. Graphical User Interface (Tkinter):

The user interacts with the system via a graphical interface built with Tkinter. This interface displays the system status, allows users to manage settings, and provides real-time monitoring of the detection process. The GUI makes it easy for non-technical users to manage alerts and view activity logs.

This architecture ensures a robust and scalable system that can function in various environments, including homes, businesses, and public spaces. It integrates real-time video analysis, machine learning-based detection, and automated alerting mechanisms for proactive security management.

B. Prerequisites

To set up and run the suspicious activity detection system, several software and hardware requirements must be fulfilled. Below is a list of the essential prerequisites for the project:

1. Hardware Requirements:

- **Camera**: A webcam or an IP camera is necessary to capture real-time video feed.
- **Microphone**: A microphone is needed for any audio-related features (optional for phone call simulation).
- **Computer**: A system with a good processor (preferably with a GPU if using complex TensorFlow models) and adequate RAM (at least 8GB) for real-time processing.
- **Network Connectivity**: For sending email alerts and simulating phone calls, an active internet connection is required.

2. Software Requirements:

➢ **Python (3.x):** Python is the primary programming language for this project.

➢ **Libraries:**

- **OpenCV:** Used for real-time video capture and image processing.
  - **Install with:** pip install opencv-python
- **TensorFlow:** Required for loading and running the pre-trained object detection model.
  - **Install with:** pip install tensorflow
- **PyAudio:** For handling audio input/output for the simulated phone call feature.
  - **Install with:** pip install pyaudio

- **Tkinter:** For creating the graphical user interface (usually pre-installed with Python).

➢ **Security Tools:**

- Intrusion Detection Systems (IDS) like Snort or Suricata, or other tools that can be integrated into the suspicious activity detection framework.
- Threat Intelligence Platforms (TIP) for external threat data integration.

3. Operating System:

The project is cross-platform and can run on Windows, macOS, or Linux. However, some library configurations may vary between operating systems (e.g., PyAudio installation).

4. Data Sources:

To train models and detect suspicious activities, your system needs access to relevant data sources:

- **Historical Data**: Logs of user activities, network traffic, or previous security incidents for analysis and testing.
- **Real-Time Data**: Continuous streams of current activity logs, network traffic, or system logs.
- **Threat Intelligence Data**: External threat feeds or signature databases that contain known attack vectors, IP blacklists, and behavioral patterns.

5.Knowledge and Expertise:

To build the system effectively, a team or individual will need expertise in the following areas:

- **Cybersecurity Concepts**:
Understanding of **anomalous behavior**, security breaches, hacking techniques, malware, and common suspicious activities to effectively define what the system needs to detect. Familiarity with **Security Information and Event Management (SIEM)** platforms for integrating logs and events.
- **Data Science and Machine Learning**:
Proficiency in feature engineering, model training, and tuning machine learning models for anomaly detection. Knowledge of supervised or unsupervised learning techniques for detecting outliers and abnormal behavior.
- **Software Development**:
Skills in backend development (e.g., API creation, database handling). Experience with event-driven architecture, microservices, and scalable design patterns for real-time detection.

c. Objectives

- One of the primary objectives is to develop a system capable of identifying suspicious activities in real time. The system should mon itor user behavior, network traffic, and system logs to promptly detect anomalies and unauthorized actions.
- Ensuring that the system can distinguish between legitimate and suspicious activity is critical. The objective is to minimize false positives and negatives, improving the accuracy of detection.
- The project aims to enable automated responses when a suspicious activity is detected, reducing the time required for human intervention and enhancing the overall security posture.
- Another objective is to provide a user-friendly interface that security administrators and non-technical users can navigate easily. The system should be intuitive enough to require minimal training.
- The system should be adaptable to different environments and scalable to monitor a wide range of activities across networks of varying sizes. It must be capable of handling different data sources and growing with the organization's needs.
- A key challenge in security systems is the generation of false alerts. One of the objectives is to fine-tune the detection algorithms so that the system minimizes false positives (incorrectly labeling benign activities as suspicious) and false negatives (missing actual threats).

VI. RESULTS

Expected results include accurate and real-time detection of suspicious activities or objects (such as unauthorized persons, abandoned objects, or unusual movements) in monitored areas.

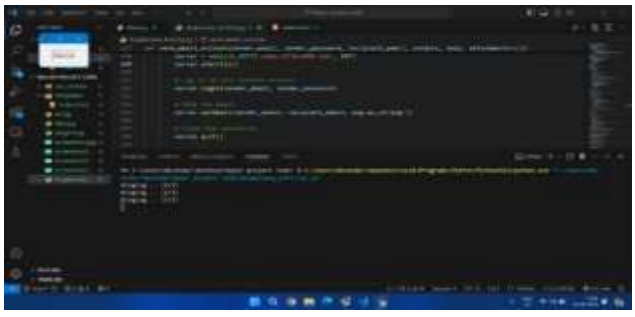

Fig:2The performance of the detection can be measured by metrics like:

- **Detection accuracy**: How well the system identifies correct objects or behaviors.
- **False positives/negatives**: Instances where the system incorrectly identifies harmless actions as suspicious or fails to detect actual threats.

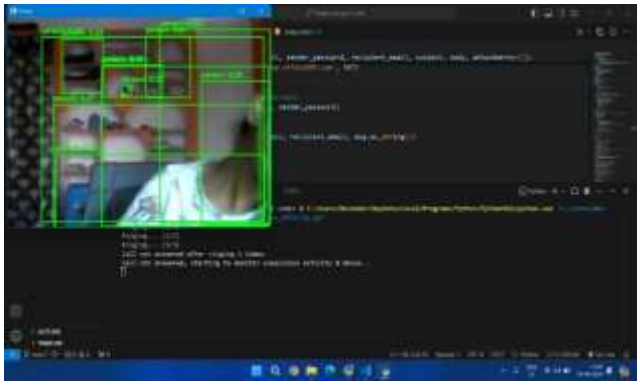

Fig:3

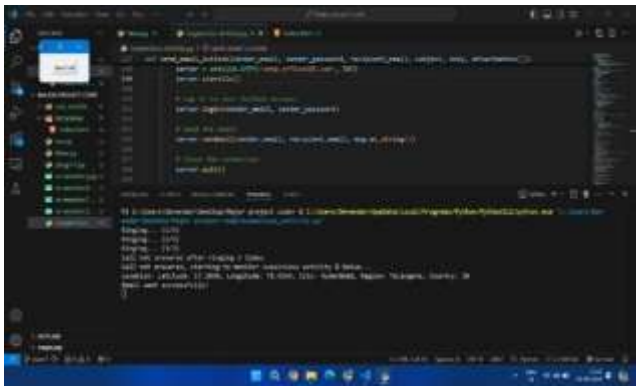

Fig:4

Upon detecting a suspicious event, the system successfully triggers an alert mechanism. The script uses smtplib to send automated email alerts, including relevant information or captured evidence (e.g., screenshots or video snippets)(fig5). Expected results would include:

- Timely delivery of emails.
- Proper attachment of any files or reports.

Fig:5

VII. CONCLUSION

The Suspicious Activity Detection and Alert System successfully demonstrates how modern technologies like computer vision and machine learning can be applied to enhance security and monitoring in real-time. By utilizing a TensorFlow-based object detection model alongside OpenCV, the system is able to analyze video feeds and detect potential threats or suspicious activities with a reasonable degree of accuracy.

In addition, the integration of automated email alerts and phone call simulations provides a robust alert mechanism, ensuring that potential risks are communicated swiftly to relevant authorities or users. This system has the potential to be implemented in various security-sensitive environments, such as public spaces, workplaces, or residential areas, where real-time detection and response are crucial.

Overall, the project proves to be a valuable step towards improving security measures through technology, showcasing the potential of AI-driven monitoring systems in protecting assets and ensuring safety.

VII. ACKNOWLEDGEMENT

We would like to express our sincere gratitude to everyone who contributed to the successful completion of the **Enhancing video call safety without alerting recipients** project.

First, we extend our heartfelt thanks to our project mentor(s) and instructor(s) for their invaluable guidance, continuous support, and encouragement throughout the development process. Their expertise in computer vision, machine learning, and system design was instrumental in shaping the core functionalities of this project.

We are also thankful to the development teams behind the libraries and tools utilized, including TensorFlow, OpenCV, and the Python community, whose open-source contributions made it possible to build an advanced and efficient system. Special thanks go to the TensorFlow developers for providing the object detection model that forms the foundation of our project. Lastly, we would like to acknowledge our peers, friends, and family members for their encouragement and feedback during various stages of development. Their support was crucial to the successful implementation and testing of the system.

Thank you to everyone who played a part in making this project a reality.

VII. REFERENCES

[1] Ong J (2013) 6 messaging services with apps for desktop andmobile https://thenextweb.comapps/2013/09/14/6-cross-platform-messaging-services-that-work-from-desktop-to-mobile/

[2] Price D (2017) 5 Online instant messaging services to chat with friends, October, 2017. https://www.makeuseof.com/tag/5-download-free-ways-to-im/

[3] Aalaap Ghag, TOP 10 WEB-BASED INSTANT MESSENGERS, NOVEMBER, 2006, https://

[4] www.firstpost.com/tech/news-analysis/ top-10-web-based-instant-messengers-3550471.html

[5] Baldikov N (2019) Everything you need to know about video conferencing, September, 2019. https://www.business2community.com/communications/everything-you-need-to-know-about-video-conferencing-02237967

[6] Zorabedian J (2014) Yes, your smartphone camera can be used to spy on you, March, 2014. https://nakedsecurity.sophos.com/2014/05/28/yes-your-smartphone-camera-can-be-used-to-spy-on-you/

[7] How to use your phone as a Webcam, November, 2014. https://gadgets.ndtv.com/mobiles/features/how-to-use-your-phone-as-a-webcam-617643

[8] Gordon W (2020) How to turn your smartphone into a wireless webcam, April, 2020. https://www.pcmag.com/how-to/how-to-turn-your-smartphone-into-a-wireless-webcam

[9] Morgan T (2020) Step by step: how to make a video call on your computer or smartphone, March, 2020. https://www.which.co.uk/news/2020/03/step-by-step-how-to-make-a-video-call-on-your-computer-or-smartphone/

[10] Imo apps pros and cons on video calls, February, 2017. https://www.techulator.com/experts/5043-imo-apps-pros-and-cons-on-video-calls

[11] Dunagan J, Liebhold M (2009) The future of real-time video communication, November, 2009. https://www.iftf.org/uploads/media/SR1278_RealtimeVideoCommunication_2.12sm.pdf

[12] Jahnavi Chowdary G, Palani Kumar S (2019) Advance control scheme for correction of power factor and voltage stability by using electric spring. Int J Innov Technol Explor Eng 8(4):337–342

[13] More AR, Prasad MSG, Wankhede Vishal A (2019) Optimized throughput and minimized energy consumption through clustering techniques for cognitive radio network. Int J Innov Technol Explor Eng 8(4S2):474–479

[14] Gaille B (2015) Skype Pros and Cons, July 2015. https://brandongaille.com/14-skype-pros-and-cons/

[15] Sai Prasanthi M, Katragadda VB, Perumalla H, Sowmya B (2019) Hybrid approach for securing the IoT devices. Int J Innov Technol Explor Eng 8(4):147–151

[16] Hrushikesava Raju S, Lakshmi Ramani B, Warris SF, Kavitha S, Dorababu S (2020) Smart eye testing. In: ISCDA-2020, October, 2020. Springer, Berlin. https://doi.org/10.1007/978-981-33-6176-8_19

[17] Hrushikesava Raju S, Burra LR, Waris SF, Kavitha S, Dorababu S (2021) Smart eye testing, advances in intelligent systems and computing. In: ISCDA 2020, 1312 AISC, pp 173–181. https://doi.org/10.1007/978-981-33-6176-8_19

[18] Kavitha M, Hrushikesava Raju S, Waris SF, Koulagaji A, Smart gas monitoring system for home and industries smart gas monitoring system for home and industries. IOP Conf Ser Mater Sci Eng 981(2). https://doi.org/10.1088/1757-899X/981/2/022003

[19] Kavitha M, Anvesh K, Arun Kumar P, Sravani P (2019) IoT based home intrusion detection system. Int J Recent Technol Eng 7(6):694–698

.