Detecting Suspicious activity in ATM

ONKAR PANCHAKSHARI[1], KARAN NIKAM[2], PRANAV KULKARNI[3], SHARDUL MAHAJAN[4]
[1, 2, 3, 4] *Student, Department of Computer Engineering, Sinhgad Institute of Technology Lonavala, Maharashtra, India.*

***Abstract—* Automated Teller Machines (ATMs) serve as crucial touchpoints for financial transactions worldwide, making them susceptible to various security threats and criminal activities. To mitigate these risks, ATM video surveillance has become an indispensable tool for enhancing security and protecting customers. This abstract provides an overview of the key aspects of ATM video surveillance, its purpose, methods, and significance in ensuring the safety of ATM users and the integrity of financial transactions.**

***Index Terms-* Detecting Suspicious activity in ATM, Video Surveillance, Safety of ATM, Security, Safety of ATM.**

I. INTRODUCTION

Problem definition:
The problem statement of the project or our goal is to detect suspicious activity in ATM and prevent crime. This project will entail detecting suspicious human Activity from real-time CCTV footage. Alert Generation On Detection Of Suspicious Activity Using Transfer Learning.

Problem objective:
Problem objective is To design an system for automatic classification of videos of single person to multi people and hence detect strange and suspicious activities. To trigger an alarm in real time, if the identified activity is suspicious.

II. METHODOLOGY

SDLC Models stands for Software Development Life Cycle Models. In this article we explore the most widely used SDLC methodologies such as Agile . Each software development life cycle model starts with the analysis, in which the Also, here are defined the technologies used in the project, team load. One of the basic notions of the software development process is SDLC models which stands for Soft- ware Development Life Cycle models. SDLC – is a continuous process, which starts from the moment, when it's made a decision to launch the project, and it ends at the moment of its full remove from the exploitation. There is no one single SDLC model. They are divided into main groups, each with its features and weaknesses.

III. SYSTEM INFORMATION

The application is designed in modules where errors can be detected and fixed easily. This makes it easier to install and update new functionality if required The Performance of the functions and every module must be well. The overall performance of the software will enable the users to overall performance of the software will enable the users to work efficiently. Performance of response should be fast. Performance of the providing virtual environment should be fast.
Programming Language: Python
Operating System: windows 10

User Interface: Application Based On Driver Condition detection

IV. SYSTEM ANALYSIS

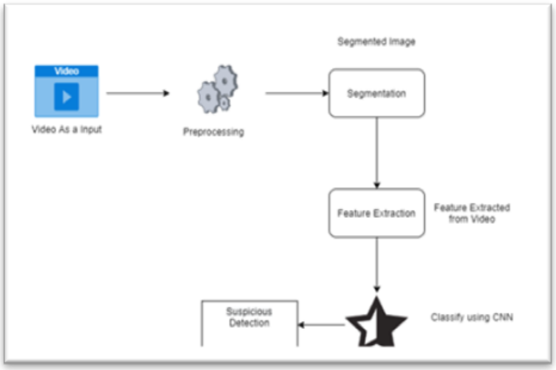


Figure 1: System Architecture

1. Data Flow Diagram: In Data Flow Diagram, we Show that flow of data in our system in DFD0 we

show that base DFD in which rectangle present input as well as output and circle show our system,

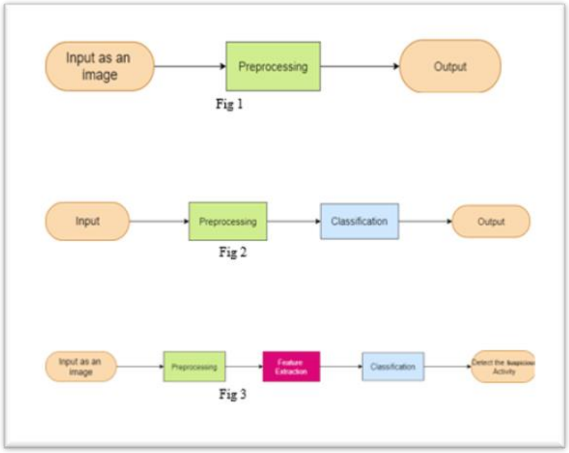


Figure 2: Data Flow

2.UML Diagram:

Unified Modelling Language is a standard language for writing software blueprints. The UML may be used to visualize, specify, construct and document the artifacts of a software intensive system is process independent, although optimally it should be used in process that is use case driven, architecture-centric, iterative and incremental. The Number of UML Diagram is available

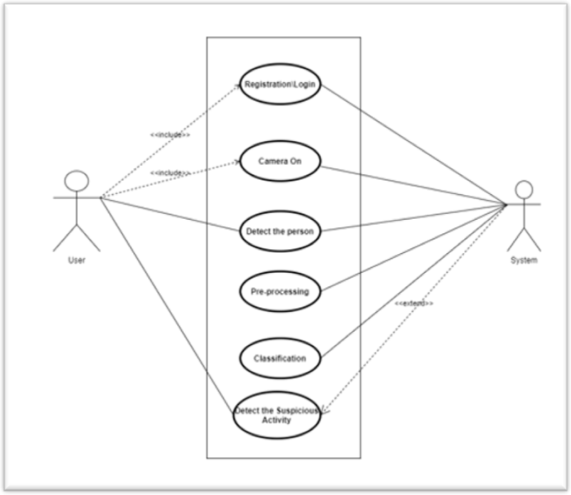


Figure 3: UML Diagram

3.Sequence Diagram: UML Sequence Diagrams are interaction diagrams that detail how operations are carried out. They capture the interaction between objects in the context of a collaboration. Sequence Diagrams are time focus and they show the order of the interaction visually by using the vertical axis of the diagram to represent time what messages are sent. This sequence diagram outlines the workflow for a surveillance or security system designed to detect suspicious activity using image processing techniques. The process starts with user authentication, followed by real-time image capture and analysis, leading to the detection of potential threats based on specific criteria.

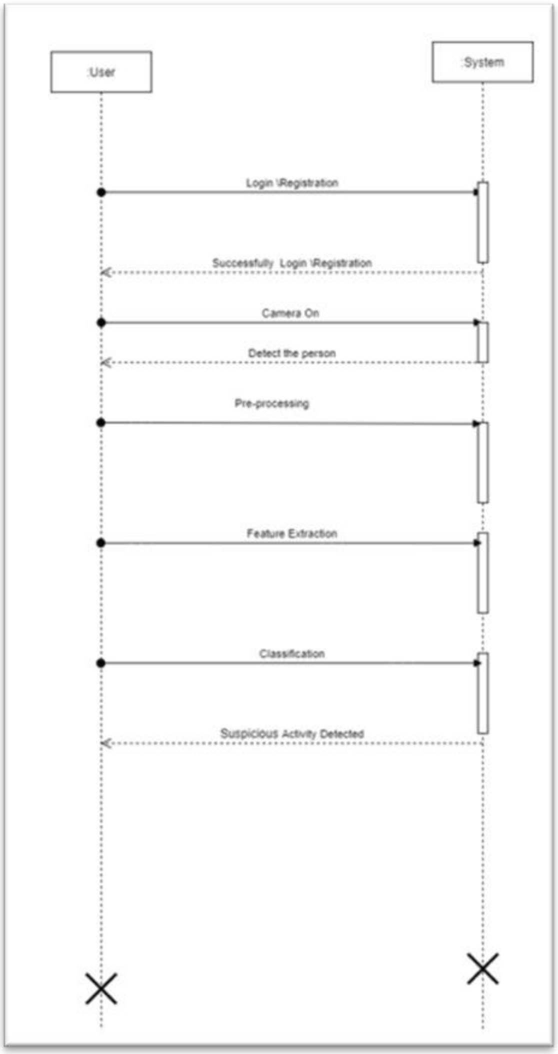


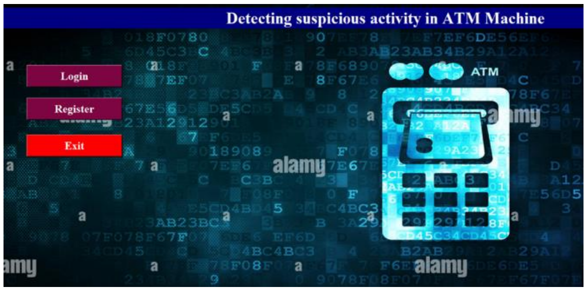
Figure 4: Sequence Diagram

ACKNOWLEDGMENT

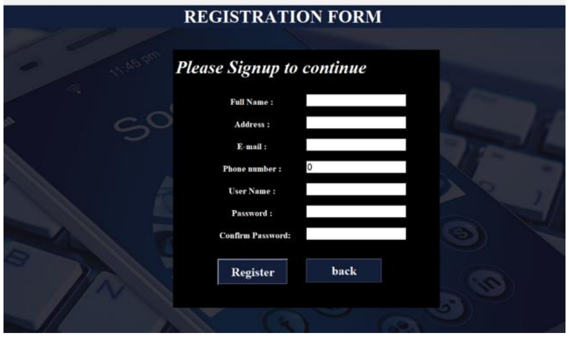
Our thanks to the Professors, experts and other faculty members who provided useful resources and background to complete this research paper. Special Contribution of Project guide Prof.B.L.Dhote madam.

The Success and outcome of this project were possible by the guidance and support from many people. We are incredibly privileged to have got this all along with the achievement of this paper. It required a lot of effort from each individual involved in this research paper. Support provided by sinhgad institute for the project made it possible for project completion.

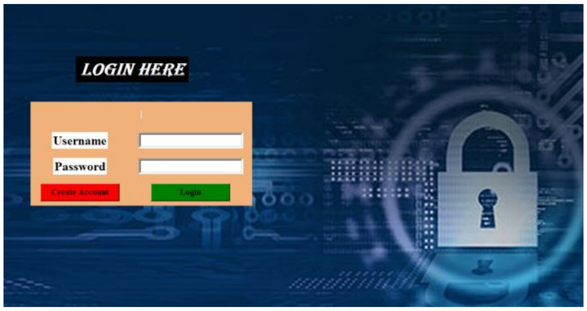
VI. RESULTS



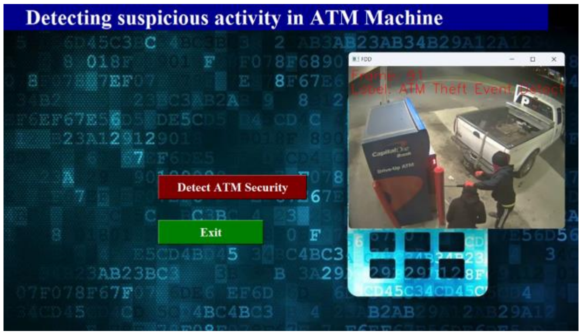
Home Page



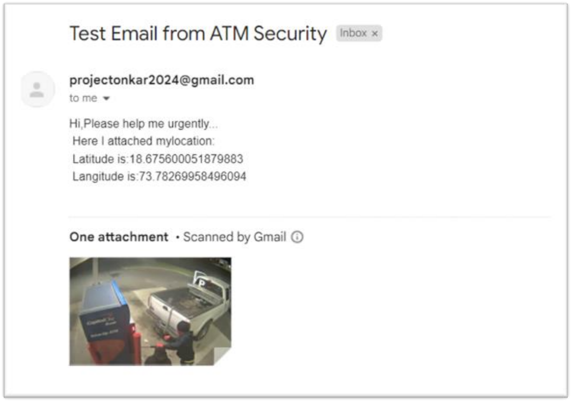
Registration Page



Login Page


Detecting suspicious activity in ATM Machine
FDD
Frame: 91
Label: ATM Theft Event Detect
Detect ATM Security
Exit

Detecting Suspicious activity



Test Email from ATM Security

projectonkar2024@gmail.com
to me

Hi,Please help me urgently...
Here I attached mylocation:
Latitude is:18.675600051879883
Langitude is:73.78269958496094

One attachment • Scanned by Gmail

Send alert to Reciever_Email

CONCLUSION

In conclusion, detecting suspicious activity in Automated Teller Machines (ATMs) using transfer learning represents a powerful and versatile approach to enhancing security, preventing fraud, and ensuring the safety of ATM users. Transfer learning leverages the capabilities of pre-trained deep learning models to adapt to the specific requirements of ATM surveillance, offering numerous advantages such as improved model performance, reduced data requirements, and faster training. Despite the undeniable benefits, there are also limitations and challenges associated with this approach, including domain mismatch, the need for annotated data, potential overfitting, and privacy concerns. However, with careful consideration and the right adjustments, many of these challenges can be effectively addressed.

The applications of suspicious activity detection in ATMs using transfer learning are diverse and impactful, ranging from fraud detection to cash trapping identification, loitering detection, and customer safety. Such systems serve as a valuable tool for financial institutions, security providers, and law enforcement agencies in their efforts to combat criminal activities and protect ATM users.As the threat landscape continues to evolve, the ongoing development and adaptation of transfer learning models for ATM surveillance will be critical. By continuously improving the technology, addressing limitations, and staying abreast of emerging threats, the financial industry can maintain the security and integrity of ATM services while instilling trust in customers and clients.In essence, transfer learning in ATM surveillance is a dynamic and promising field that offers a robust solution to security challenges, making ATM transactions more secure and contributing to the overall well-being of individuals and organizations

FUTURE SCOPE

The future scope of ATM video surveillance for monitoring and detecting suspicious activities is likely to see significant advancements as technology continues to evolve. Here are some key areas of development and potential trends in the future of ATM video surveillance.

REFERENCES

[1] P. Bhagya Divya, S .Shalini , R .Deepa , Baddeli Sravya Reddy ,“Inspection of suspicious human activity in the crowdsourced areas captured in surveillance cameras” , International Research Journal of Engineering and Technology (IRJET), December 2017.

[2] Jitendra Musale , Akshata Gavhane , Liyakat Shaikh, Pournima Hagwane , Snehalata Tadge , “Suspicious Movement Detection and Tracking of Human Behavior and Object with Fire Detection using A Closed Circuit TV (CCTV) cameras ”, International Journal for Research in Applied Science & Engineering Technology (IJRASET) Volume 5 Issue XII December 2017.

[3] U. M. Kamthe , C . G .Patil “Suspicious Activity Recognition in Video Surveillance System”, Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), 2018.

[4] Zahraa Kain, Abir Youness, Ismail El Sayad, Samih Abdul-Nabi, Hussein Kassem, “ Detecting Abnormal Events in University Areas ”, International conference on Computer and Application,2018.

[5] Tian Wanga, Meina Qia, Yingjun Deng, Yi Zhouc, Huan Wangd, Qi Lyua, Hichem Snoussie, “Abnormal event detection based on analysis of movement information of video sequence” ,Article-Optik,vol-152,January-2018.