EXPLAINABLE AI WITH A BLOCKCHAIN-ENABLED PUBLIC SAFETY SOLUTION

A Project Report Submitted

in Partial Fulfilment of the Requirements

for the Degree of

Bachelor of Technology

in

Computer Science and Engineering

by

PALASH RAWAT-2020BCS0057

DOMMATI MANIKANTA-2020BCS0030

ADITYA SHITALE-2020BCS0082

RAUNAK KUMAR-2020BCS0124

to

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

INDIAN INSTITUTE OF INFORMATION TECHNOLOGY

KOTTAYAM-686635, INDIA

April 2024

DECLARATION

We, **BTP Group 42**, hereby declare that, this report entitled **"Explainable AI with a blockchain-enabled Public safety solution"** submitted to Indian Institute of Information Technology Kottayam towards partial requirement of **Bachelor of Technology** in **Computer Science and engineering** is an original work carried out by me under the supervision of **Dr. Ebin Deni Raj** and has not formed the basis for the award of any degree or diploma, in this or any other institution or university. I have sincerely tried to uphold the academic ethics and honesty. Whenever an external information or statement or result is used then, that have been duly acknowledged and cited.

Kottayam-686635	**PALASH RAWAT**
November 2023	**DOMMATI MANIKANTA**
	ADITYA SHITALE
	RAUNAK KUMAR

ACKNOWLEDGMENT

we would like to express our heartfelt gratitude to Dr. Ebin Deni Raj for his exceptional guidance, mentorship, and unwavering support throughout our Bachelor's Thesis Project (BTP). Dr. Raj's expertise, valuable insights, and continuous encouragement have been instrumental in shaping the direction and success of our project.

We extend our sincere thanks to the esteemed panel members, Dr. Bhanu Chander and Dr. Shajuline Benedict, for their invaluable contributions. Their thoughtful reviews, constructive feedback, and guidance during every phase presentation have significantly enriched our work and helped us navigate challenges effectively.

We are grateful for the opportunity to learn from such distinguished scholars and mentors who have dedicated their time and expertise to ensure our academic and professional growth. Their support has been pivotal in our journey, and we deeply appreciate their contributions to our project's development and success.

PALASH RAWAT
DOMMATI MANIKANTA
ADITYA SHITALE
RAUNAK KUMAR

CERTIFICATE

This is to certify that the work contained in this project report entitled **“Explainable AI with a blockchain-enabled Public safety solution”** submitted by **BTP Group 42** to the Indian Institute of Information Technology Kottayam towards partial requirement of **Bachelor of Technology** in **Computer Science and Engineering** has been carried out by group under my supervision and that it has not been submitted elsewhere for the award of any degree.

Kottayam-686635
November 2023

(Dr. Ebin Deni Raj)
Project Supervisor

ABSTRACT

In today's digital age, ensuring public safety is paramount, requiring innovative solutions that integrate cutting-edge technologies. Our B.Tech project introduces a novel approach merging Explainable Artificial Intelligence (AI) with blockchain technology to bolster public safety measures. The primary objective of our project is to enhance public safety by detecting anomalies in CCTV footage, even in low-resolution scenarios.

Our methodology involves training a robust AI model on CCTV footage data, adept at identifying anomalies indicative of potential threats or irregularities. Leveraging the power of SHAP (SHapley Additive exPlanations) technology, our project provides explainability, offering insights into the decision-making process of the AI model. This feature empowers developers and stakeholders to comprehend why a particular decision was made, enhancing transparency and trust in the system.

Furthermore, we integrate blockchain technology into our solution to ensure the integrity and authenticity of detected anomalies. By securely recording detected anomalies on a blockchain network, we provide an immutable and transparent record accessible to relevant authorities.This not only enhances data security but also facilitates streamlined collaboration among stakeholders.

Overall, our project represents a significant advancement of public safety, offering a comprehensive solution that combines AI with blockchain technology while prioritizing explainability. By providing accurate anomaly detection, transparency in decision-making, and secure data management, our solution aims to the enhancement of public safety protocols.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

This project seeks to ensure the safety and protection of the general population. Specifically, we are developing a model that will detect anomalies in cctv footage using videos or images to identify violations. The model will then send this information via blockchain to the nearby police station. Most studies so far have focused on just one thing, such as developing a knife or gun detection. Detection also requires high-resolution videos or photos to train the model, but that won't always be the case, thus our project will detect anomalies in all areas of operation [1].

1.1 Significance :

Public Safety: Ensuring the safety of the general population is a fundamental responsibility of any society. Your project directly contributes to this by using technology to identify potential threats or violations in public spaces. **Comprehensive Anomaly Detection:** Unlike many existing projects that focus on specific types of anomalies (like weapons detection), our project aims to detect a wide range of violations.

Versatility in Data Input: Acknowledging the limitations of high-resolution footage, this project aims to work with a variety of input data, including both images and videos.

Blockchain Integration for Data Security: The incorporation of blockchain technology adds an additional layer of security to the project. It ensures that the data remains tamper-proof and is securely transmitted to the appropriate authorities.

Potential for Scalability and Replicability: there is considerable potential for it to be scaled to various environments and seamlessly integrated with existing surveillance systems. This could lead to a significant enhancement of public safety measures on a broader scale. **Protection of Privacy:** While the project's primary goal is to identify potential threats, it's important to ensure that privacy rights are respected.

1.2 Motivation

India stand 77th in the crime rate in the whole world. The latest crime rate report of India in 2023 reveals a marginal decrease of 0.56 percent in the overall crime rate compared to the previous year. However, certain specific crimes have exhibited an increase in reported incidents. Our motivation is to encounter this situation through the modern techniques,like AI and blockchain. AI has become increasingly important in this period, and public safety is a significant concern where AI can play a crucial role in reducing crime rates and incidents.

1.3 Architecture and Working

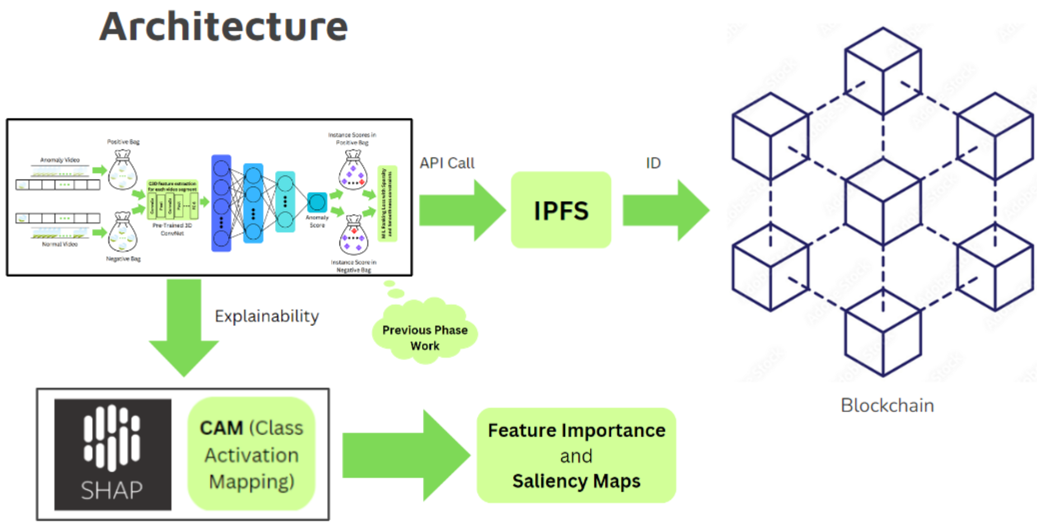

Architecture
Anomaly Video
Positive Bag
C3D feature extraction for each video segment
Pre-Trained 3D ConvNet
Normal Video
Negative Bag
Anomaly Score
Instance Scores in Positive Bag
Instance Score in Negative Bag
MIL Ranking Loss with Sparsity and Smoothness constraints
API Call
IPFS
ID
Blockchain
Explainability
Previous Phase Work
SHAP
CAM (Class Activation Mapping)
Feature Importance and Saliency Maps

Figure 1.1: Complete Architecture

Features :-

Decentralized Storage: Images are uploaded to IPFS, ensuring decentralized and immutable storage.

Smart Contract: Utilizes Solidity smart contracts on the Ethereum blockchain for access control and ownership management.

Access Control: Users can grant or revoke access to their uploaded images to specific individuals through the smart contract.

Technologies Used :-

Solidity: Smart contract development for ownership and access control.

React: Front-end interface for uploading images and managing access.

IPFS: Decentralized storage protocol for hosting uploaded images.

Usage, working and significance :-

1. **Machine Learning Model for Anomaly Detection:** We developed a machine learning model specifically designed to detect anomalies. This model is likely trained on a dataset to recognize patterns that deviate from the norm.

2. **Integration with Blockchain Technology:** The detected anomalies, along with associated images and reports, are seamlessly integrated with a blockchain. Blockchain ensures the security, transparency, and immutability of the data by creating a decentralized and tamper-resistant.

3. **Inclusion of Images and Reports in Blockchain:** The images and reports related to the detected anomalies are added as transactions or data entries to the blockchain.

4. **Access Control Mechanism:** Access to view the stored images and reports is controlled through a defined access control mechanism. This ensures that only authorized individuals or entities have the privilege to access and review the anomaly-related information.

5. **Immutable Record Keeping:** The integration of blockchain ensures an immutable record of all activities. Any changes or additions to the access permissions or data are securely documented, providing a reliable and auditable history.

6. **Explainability aspect:** Explaining machine learning models with Shapley values. Shapley values are a widely used approach from cooperative game theory that come with desirable properties. [2]

Chapter 2

Literature Survey

This chapter includes all the literature survey that was done while developing robust and reliable AI model integrated with blockchain for public safety.

2.1 Literature Survey

The integration of blockchain and deep learning has led to innovative frameworks like BlockCrime, a collaborative intelligence system aimed at enhancing public safety by detecting malicious activities.[3] The BlockCrime framework utilizes a Convolutional Neural Network (CNN) based Xception model, achieving a high accuracy rate of 96.57% in crime detection. This approach not only alerts law enforcement agencies but also securely stores crime scenes using blockchain technology, showcasing the potential of combining deep learning and blockchain for societal benefits.

Another application of deep learning and blockchain is in identifying risks in low-frequency, high-value situations. [4] By encrypting and aggregating firm data into training programs using blockchain technology, deep learning algorithms can provide early warnings for potential risks. This strategy not only addresses the challenge of ”small training” data but also leverages blockchain’s secure and immutable nature to enhance risk management capabilities within organizations.

The significance of integrating blockchain with deep learning is further explored in a literature review that delves into existing frameworks and their potential for informed decision-making. [5] This review classifies blockchain integration based on various criteria and evaluates the strengths and weaknesses of current blockchain-based deep learning frameworks. It highlights the ongoing research challenges in constructing reliable deep learning systems integrated with blockchain, emphasizing the need for continued exploration and development in this field.

In the context of video surveillance, an optimized deep learning framework is proposed for crime activity prediction. This framework aims to detect suspicious activities without determining the appropriate action to take based on the observations. It reflects the ongoing efforts to leverage deep learning techniques for enhancing security and surveillance systems, showcasing the potential for advanced AI-based solutions in crime prevention and detection. [6]

The use of blockchain technology in CCTV surveillance systems addresses concerns related to data integrity and security. By implementing a data verification system using blockchain, smart cities can ensure the authenticity and tamper-proof nature of surveillance data. While this approach offers significant benefits in terms of data security, scalability remains a challenge that requires further exploration and optimization in blockchain-based systems for CCTV surveillance. [7]

Advancements in explaining the decisions made by deep learning models are also noteworthy. Gradient-weighted Class Activation Mapping (Grad-CAM) is a technique widely used in the realm of deep learning and computer vision. Its primary function is to provide a visual representation of the specific regions within an image that are most heavily weighted by a convolutional neural network (CNN) during the decision-making process. This tool proves invaluable in comprehending the thought process behind the network's predictions.

Grad-CAM operates by analyzing the gradients associated with a designated target, such as identifying a 'dog' within an image classifier or a sequence of words within a captioning system. These gradients serve as indicators of the significance of each portion of the image in influencing the final outcome. Subsequently, Grad-CAM generates a rudimentary map that outlines the key areas within the image that contribute most significantly to the decision-making process.

One of the standout features of Grad-CAM is its versatility, as it seamlessly integrates with various types of CNN architectures. Whether it's a network with densely connected layers like VGG, a model designed for generating structured outputs like captions, or one handling tasks involving multiple types of input, such as visual question answering or reinforcement learning, Grad-CAM remains adaptable. What sets it apart is its ability to function without necessitating any alterations to the underlying architecture or requiring extensive retraining.

Grad-CAM++ [8] is introduced as an extension of GradCAM, aimed at providing clearer visual explanations for CNN predictions. This development reflects the ongoing efforts to enhance the interpretability and transparency of deep learning models, contributing to their trustworthiness and applicability in various domains requiring explainable AI solutions.

Chapter 3

Methodology

Our project methodology integrates several key steps to achieve CCTV anomaly detection and ensure model transparency. Firstly, we begin with data collection, where CCTV footage in MP4 format is gathered from relevant sources. To prepare this data for analysis, we employ video processing techniques using libraries like OpenCV to extract frames. These frames are sampled at regular intervals, such as every 32 frames, to maintain consistency in the dataset. Subsequently, these extracted frames are converted into NumPy (npy) format, facilitating feature extraction and analysis in later stages.

The next critical phase involves feature extraction, where deep learning-based techniques are applied to the npy files. Our approach leverages pre-trained convolutional neural network (CNN) models, such as Xception or ResNet, for efficient and effective feature extraction. Transfer learning techniques are employed to adapt these models to our specific anomaly detection task, compensating for the limited size of our dataset. This step ensures that meaningful patterns and anomalies within the video frames are accurately captured.

Following feature extraction, we develop a dedicated anomaly detection model based on deep learning principles. This model is trained using labeled data, distinguishing between normal and anomalous frames. During the inference stage, each set of extracted features is fed into the trained model, predicting the probability of an anomaly occurring within each 32-frame segment. This approach enables us to identify potential anomalies in real-time video streams, enhancing surveillance and security systems.

Moreover, to ensure model transparency and enhance explainability, we implement SHAP (SHapley Additive exPlanations) and Grad-CAM (Gradient-weighted Class Activation Mapping) methods. SHAP provides insights into feature importance, explaining the model's predictions and aiding in understanding the underlying decision-making process. Grad-CAM, on the other hand, generates heatmaps highlighting areas of interest in the input frames that contribute significantly to the model's predictions. By integrating these explainability techniques, we not only improve model interpretability but also build trust and confidence in the system's reliability for anomaly detection in CCTV surveillance. Additionally, to maintain the integrity and tamper-proof nature of our model's output, we propose integrating a blockchain network built using IPFS (InterPlanetary File System), ensuring the security and immutability of crucial data points, especially those related to anomaly spikes detected by our model.

3.1 Deep Learning Model

Deep learning, a subset of artificial intelligence (AI), has emerged as a powerful tool in various domains, including computer vision and natural language processing. In the context of crime detection, it offers a highly effective approach to analyze and interpret complex patterns in visual and textual data.

Anomaly Detection:

Deep learning models, especially recurrent neural networks (RNNs) and Long Short-Term Memory networks (LSTMs), are well-suited for anomaly detection. By training on normal behavior patterns, these models can effectively identify deviations indicative of suspicious or criminal activities. This capability is fundamental in early crime detection and prevention.

Theorem 3.1.1. *Universal Approximation Theorem:*

Proof. This theorem states that a feedforward neural network with a single hidden layer containing a finite number of neurons can approximate any continuous function on a compact subset of Euclidean space, given enough hidden units. □

3.2 Blockchain

To further bolster the credibility and effectiveness of the crime detection system, the integration of blockchain technology provides a robust foundation for data integrity and transparency. Through the use of immutable ledgers, all transactions and data manipulations within the system are recorded, ensuring the verifiability of results and preventing tampering with crucial evidence. We have used IPFS to implement Blockchain.

IPFS (Inter Planetary File System) : IPFS is a distributed and decentralized file storage protocol that enables global computers to store and share files within an extensive peer-to-peer network. Any computer in the world can download the IPFS software, which enables it to host and serve files. When someone uses IPFS on their computer, they can upload files to the network so that anyone else with IPFS installed on their system anywhere in the world can view and download them. Although some storage providers—also referred to as pinning services—are designed to support IPFS, IPFS is a protocol and not a provider. Although IPFS can be installed on cloud infrastructure and used in conjunction with it, it is not a cloud service provider in and of itself.

1. Secure and Immutable Record Keeping: - Blockchain serves as a decentralized ledger where reports generated by the AI model are stored. This ensures that once a report is recorded, it cannot be altered or tampered with, providing a high level of data integrity.

2. Transparent and Traceable Transactions: - Each report submission is recorded as a transaction on the blockchain. This transparent ledger allows for a traceable history of all interactions, including when a report was generated, who accessed it, and when it was shared with relevant authorities.

3.3 Explainable AI

XAI aspect of project using SHAP and Grad-CAM contributes to:

Transparency: Providing clear insights into the model's decision-making process, showing which features or parts of video frames influence anomaly predictions.

Interpretability: Enabling stakeholders to understand why the model flags certain segments as anomalous, enhancing trust and facilitating human-machine collaboration in interpreting and acting upon detected anomalies.

Trustworthiness: Demonstrating that the model's predictions are based on meaningful features, reducing the "black box" perception often associated with deep learning models and making the system more trustworthy and reliable for real-world applications, such as surveillance and security.

SHAP (SHapley Additive exPlanations):

SHAP is a powerful technique for explaining individual predictions of machine learning models, including deep learning models like the one used in your project. By using SHAP, system can provide insights into which features or attributes of the video data contribute more significantly to the model's anomaly detection decisions. For example, SHAP can highlight specific frames, temporal patterns, or spatial features within frames that are crucial in identifying anomalies. This information is valuable for understanding why the model flagged certain segments as anomalous, improving the system's transparency.

Grad-CAM (Gradient-weighted Class Activation Mapping):

Grad-CAM is another explainability technique that generates heatmaps to visualize which parts of an image (or video frame, in your case) are important for a model's prediction. [9] By applying Grad-CAM to anomaly detection model, you can generate heatmaps that highlight regions within video frames that the model focuses on when making anomaly predictions. These heatmaps can help stakeholders, such as security personnel or system administrators, understand the model's decision-making process by visually showing where the model ”looks” to detect anomalies. This visual explanation enhances transparency and trust in the system [10].

3.4 Working of model

1. Current Anomaly Detection Model: The statement begins by asserting the effectiveness of the existing anomaly detection model. It suggests that the model is performing well, and this claim is supported by evidence provided in a demo video.

2. Demonstration of Probability Numbers: The demo video showcases probability numbers generated by the anomaly detection model. Probability numbers are a measure of the model's confidence in its predictions.

3. Low Probability for Normal Conditions: In normal, non-anomalous situations, the model produces low probability numbers. Specifically, the mentioned range is from 0.02 to 0.2. This indicates a high degree of certainty by the model that no anomaly is present.

4. Evidence in Demo Video: The statement implies that the viewers can verify the model's performance by referring to the provided demo video. The video likely illustrates instances where the model accurately assigns low probabilities during normal conditions.

5. Probability Spike during Anomalies: When an anomaly occurs, the model's confidence level, as indicated by the probability numbers, significantly increases. The probability range mentioned is from 0.8 to 0.9. This suggests that the model is highly certain that an anomaly has occurred.

3.5 Variational autoencoder

Variational autoencoders were proposed by Knigma and Welling from Google and Qualcomm in 2013. Variational autoencoders (VAEs) provide an effective way to identify observations in the latent space. Therefore, instead of creating an encoder that outputs a value that describes each state behavior, we will create an encoder that describes the result of each hidden behavior.

Significance in project

Using Variational Autoencoders (VAEs) for anomaly detection in videos is an innovative approach that leverages the capabilities of VAEs to learn a compact representation of normal video frames. [11] Here is a step-by-step guide on how to use VAEs for video anomaly detection:

Data Preparation:

Gather a dataset of normal videos for training the VAE. These should represent typical, non-anomalous behavior. Additionally, collect a dataset of anomalous videos for testing the anomaly detection system.

Frame Extraction:

Divide each video into frames. This can be done using libraries like OpenCV in Python.

Minimize 1: $(x - \hat{x})$

Minimize 2: $\frac{1}{2}\sum_{i=1}^{n}\left(e^{\sigma_i} - (1 + \sigma_i) + \mu_i^2\right)$

3.6 Libraries

1. openCV:

OpenCV (Open Source Computer Vision Library: `http://opencv.org`) is an open-source library that includes several hundreds of computer vision algorithms

Significance: The OpenCV library is utilized in our project to detect movement in anomaly videos, ensuring swift recognition of anomalies. This library filters out stable parts of the videos, emphasizing motion, allowing our dataset to pass through this motion detection phase before proceeding to the further identification of the specific anomaly occurring.

2. TensorFlow/Keras:

OpenCV (TensorFlow is an open-source machine learning framework developed by Google. It provides a comprehensive set of tools for building and deploying various machine learning models, including deep learning models, which are particularly powerful for tasks like image recognition, anomaly detection,etc.

Significance: Deep learning models, especially recurrent neural networks

(RNNs) and convolutional neural networks (CNNs), are powerful for anomaly detection. They can learn complex patterns and detect deviations from normal behavior in data, which is essential for identifying suspicious activities in your project.

3. SHAP (SHapley Additive exPlanations):

The SHAP (SHapley Additive exPlanations) library in Python is used for explaining the output of machine learning models. It provides tools to compute Shapley values, which assign each feature an importance score in a prediction. This helps in understanding the contribution of each feature to the model's output, making it easier to interpret and debug machine learning models. SHAP can be applied to various types of models, including tree-based models, deep learning models, and more.

Significance: The SHAP (SHapley Additive exPlanations) method can be highly significant for anomaly detection models due to its ability to explain model predictions. By using SHAP, you can gain insights into why certain instances are classified as anomalies or normal data points. This interpretability can help in understanding the features and patterns that contribute most to the model's anomaly detection decisions, leading to more accurate and reliable anomaly detection systems.

Chapter 4

Experimental Results

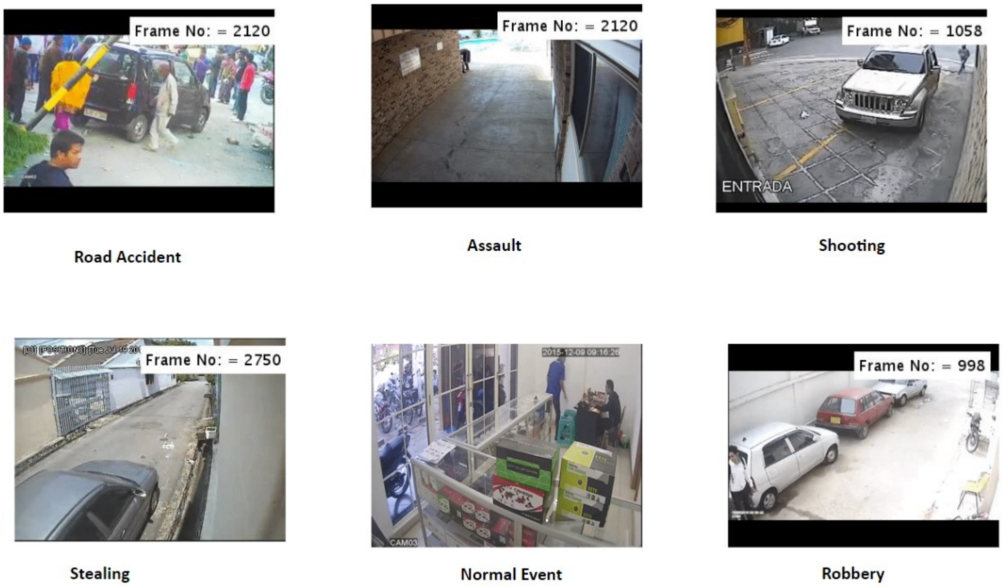
4.1 Dataset

UCF Crimes folders :

UCF has produced a new large-scale documentary called UCF-Crime, which features long-form, uncensored videos covering 13 serious global problems such as torture, arrest, fire, murder, accident, injury, theft, explosion, fight. theft, armed assault, robbery, shopping and torture. These vulnerabilities were selected for their significant impact on public safety.

	videos	Avg Frames	Dataset length	Example anomalies
UCSD Ped1	70	201	5 min	Bikers, walking across walkways, small cart
UCSD Ped1	28	163	5min	Bikers, walking across walkways, small cart,
Subway Enterance	1	121,749	1.5hours	Wrong direction, No payment
Subway Exit	1	64,901	1.5 hours	Wrong direction, No payment
Avenue	37	839	30 min	Run, throw, new object
UMN	5	1290	5 min	RUN
BOSS	12	4052	27min	Harass, disease, Panic
Ours	**1900**	**7247**	**128 hours**	**Abuse, fighting, assault, accident,burglary**

Table 4.1: Data Comparison



Road Accident

Assault

Shooting

Stealing

Normal Event

Robbery

Figure 4.1: Types of anomalies

4.2 Experimental Result

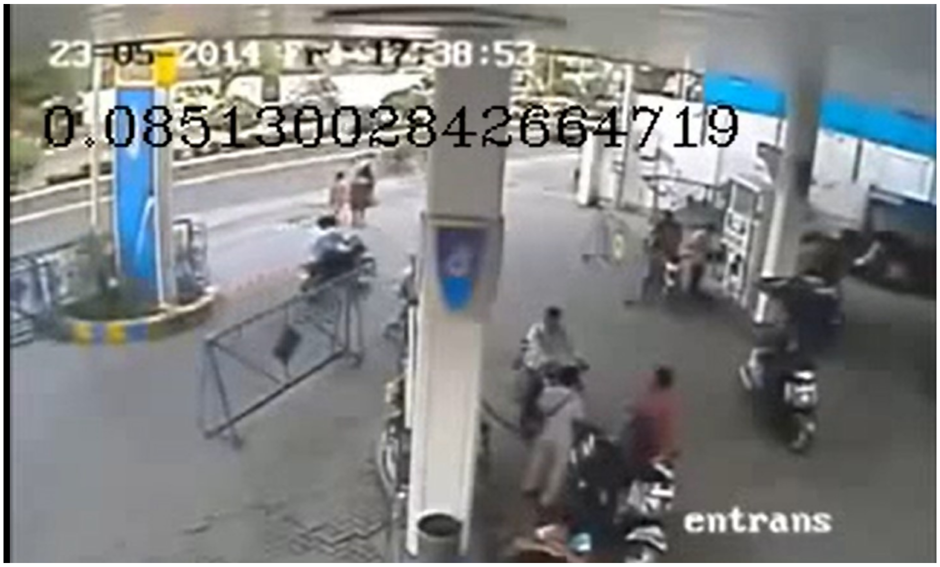


Figure 4.2: Anomaly with normal event
Normal event occuring in ccv footage and probability is low.

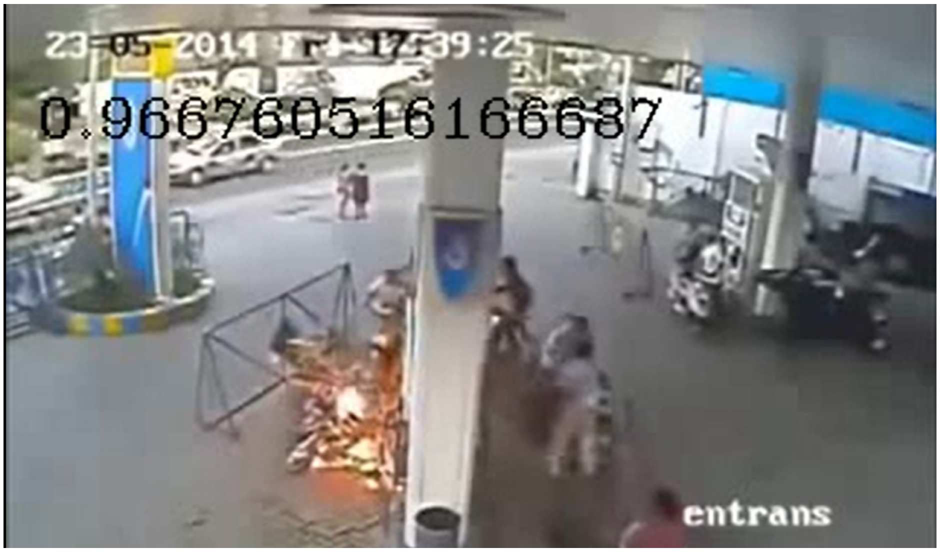


Figure 4.3: Anomaly with abnormal event
abnormal event happened in cctv and probability spiked.

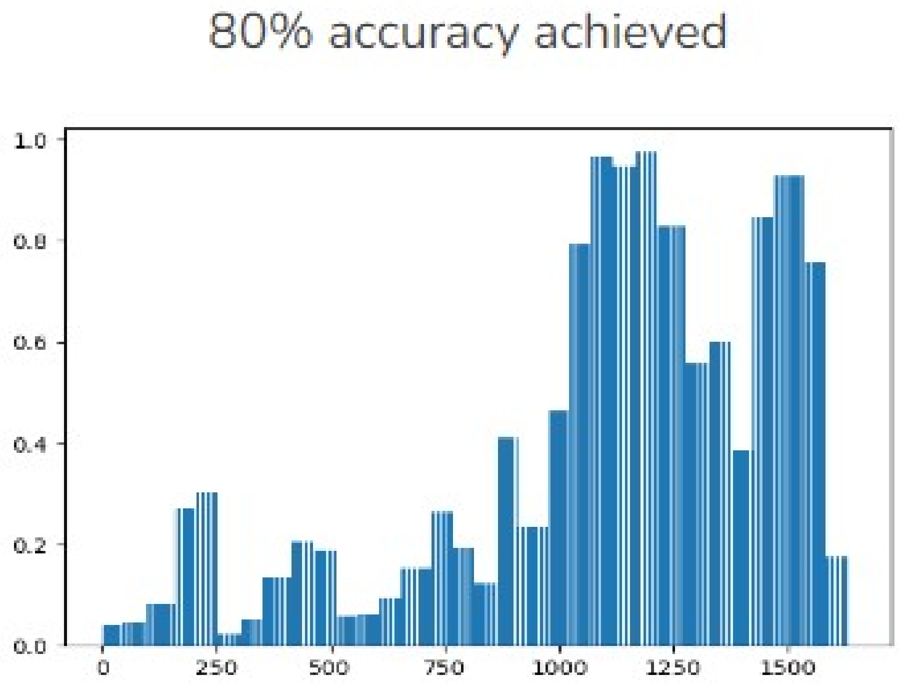


Figure 4.4: Probability distribution of anomaly vs frames in second

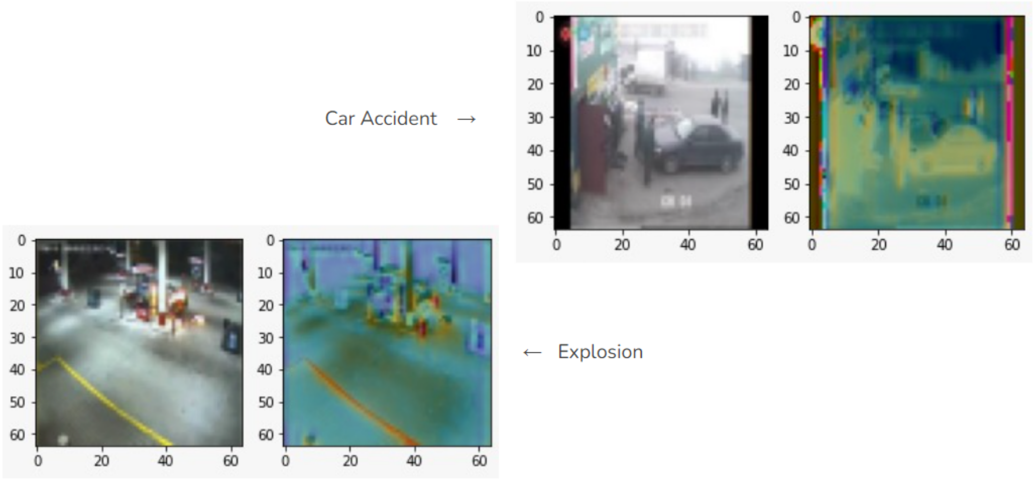
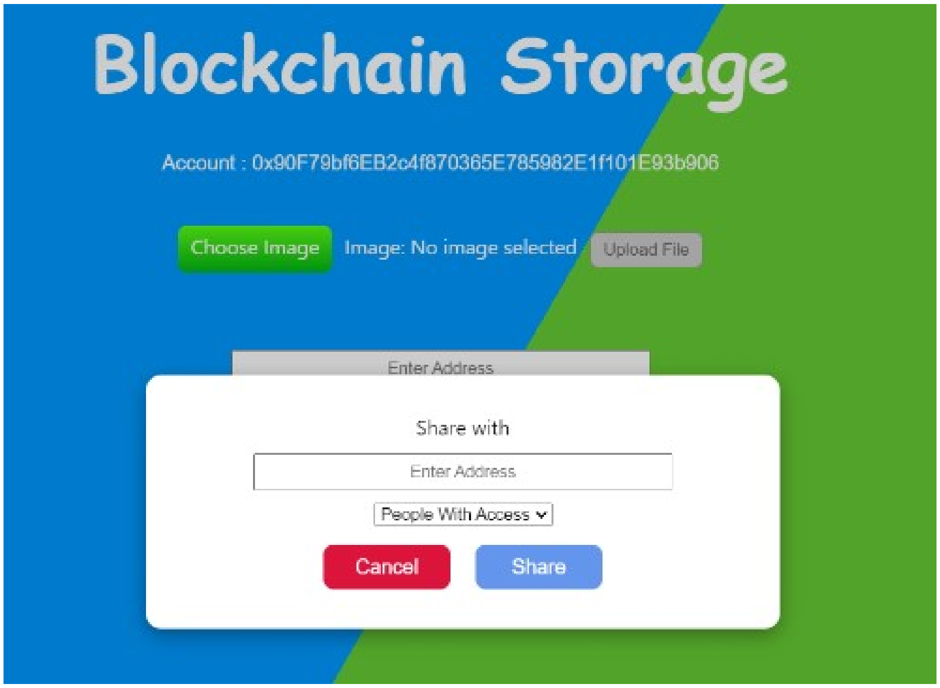


Figure 4.5: Explainability using CAM based method



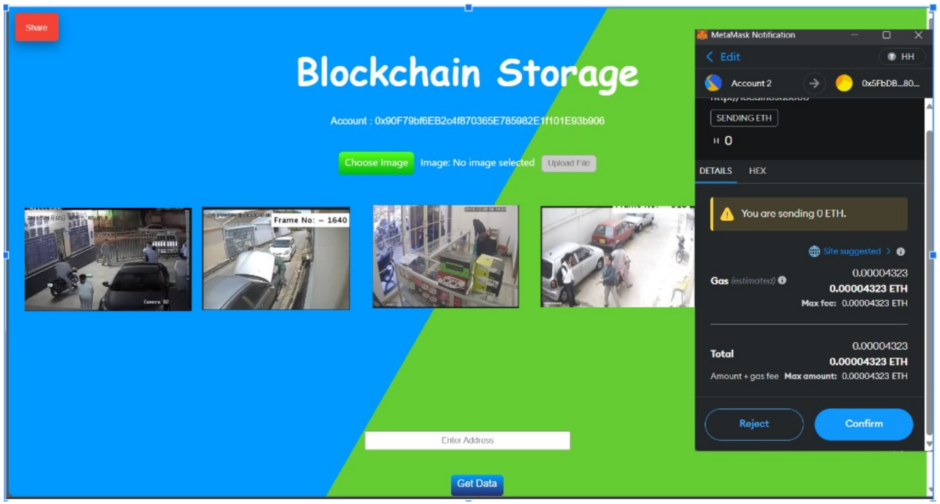
Blockchain Storage

Account : 0x90F79bf6EB2c4f870365E785982E1f101E93b906

Image: No image selected

Share with

Figure 4.6: entering anomaly files on blockchain



Blockchain Storage

Account : 0x90F79bf6EB2c4f870365E785982E1f101E93b906

Image: No image selected

MetaMask Notification

Account 2 → 0x5FbDB...80...

SENDING ETH

0

You are sending 0 ETH.

Gas (estimated) 0.00004323 0.00004323 ETH Max fee: 0.00004323 ETH

Total 0.00004323 0.00004323 ETH

Amount + gas fee Max amount: 0.00004323 ETH

Figure 4.7: Get anomaly files on blockchain

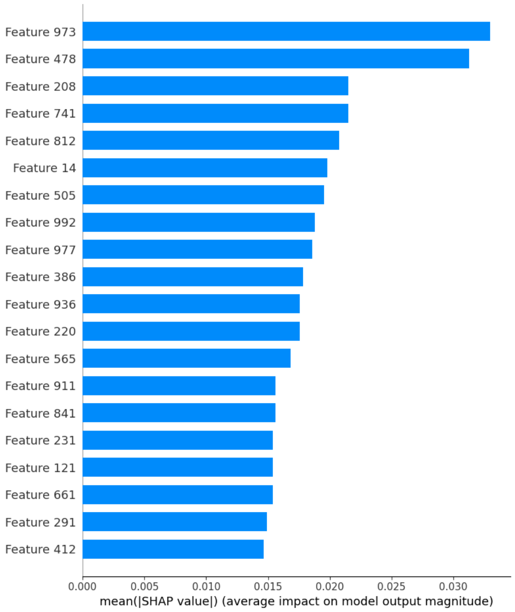


Figure 4.8: SHAP output for Explainability

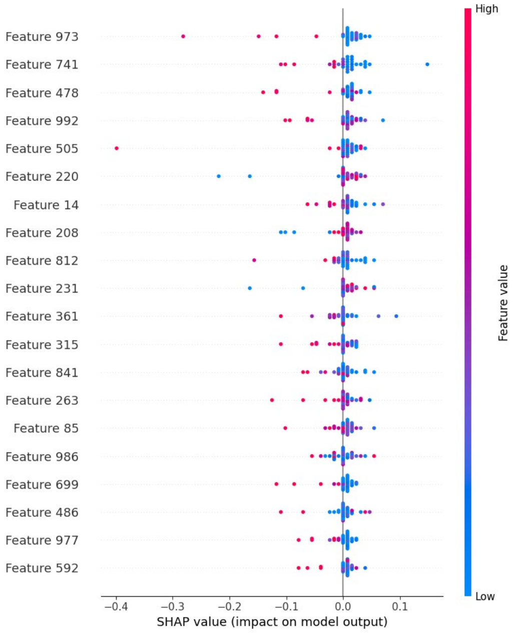


Figure 4.9: SHAP output for Explainability

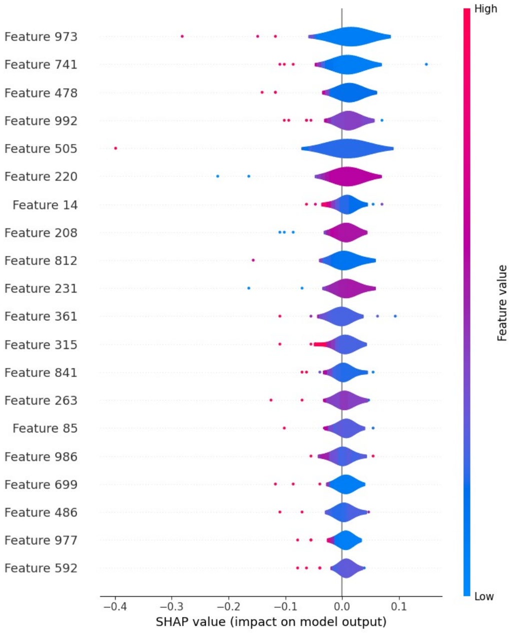


Figure 4.10: SHAP output for Explainability

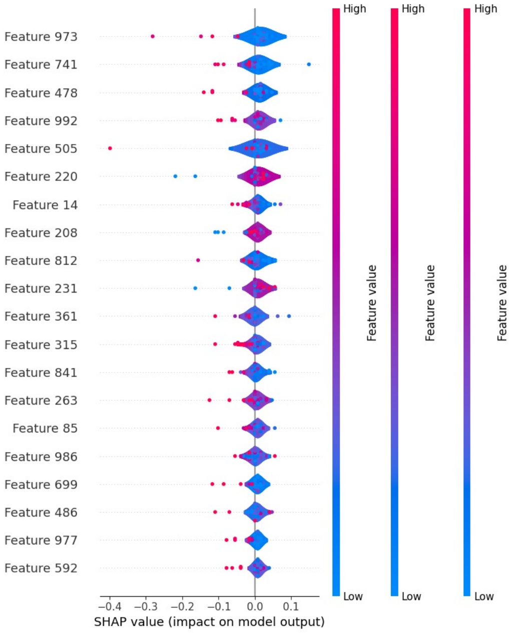


Figure 4.11: SHAP output for Explainability

Chapter 5

Conclusion and Future Work

In conclusion, our project has achieved significant milestones and delivered promising results. Our machine learning model has been successfully developed and tested, demonstrating an impressive accuracy rate of 80%. This indicates the model's effectiveness in making accurate predictions based on the input data.

Furthermore, we have implemented a robust blockchain network to store the model's outputs securely. This integration enhances data integrity, transparency, and security, aligning with modern standards of data management and privacy protection.

A key aspect of our project's success lies in the implementation of the SHAP (SHapley Additive exPlanations) library for model explainability. By employing SHAP-based methods and techniques, we have enhanced the interpretability and transparency of our model. This approach not only provides insights into feature importance but also enables stakeholders to understand the model's decision-making process with greater clarity.

The combination of a high-performing machine learning model, a secure blockchain network, and advanced explainability techniques sets a solid foundation for future developments and applications in the field. Our project emphasizes the importance of accuracy, transparency, and accountability in deploying machine learning solutions, contributing to the advancement of responsible AI practices.

Bibliography

[1] A. Javed, W. Ahmed, S. Pandya, P. Maddikunta, M. Alazab, and T. Gadekallu, "A survey of explainable artificial intelligence for smart cities," *Electronics*, vol. 12, no. 4, p. 1020, 2023.

[2] S. Kitamura and Y. Nonaka, "Explainable anomaly detection via feature-based localization," *Artificial Neural Networks and Machine Learning – ICANN 2019: Workshop and Special Sessions*, pp. 408–419, 2019.

[3] M. Shafay, R. Ahmad, K. Salah, I. Yaqoob, R. Jayaraman, and M. Omar, "Blockchain for deep learning: review and open challenges," *Cluster Computing*, vol. 26, no. 1, pp. 197–221, 2023.

[4] N. Brestoff and J. Rajagopal, "Using classified text, deep learning algorithms and blockchain to identify risk in low-frequency, high value situations, and provide early warning," 2018.

[5] D. Patel, H. Sanghvi, N. Jadav, R. Gupta, S. Tanwar, B. Florea, D. Taralunga, A. Altameem, T. Altameem, and R. Sharma, "Blockcrime: Blockchain and deep learning-based collaborative intelligence

framework to detect malicious activities for public safety," *Mathematics*, vol. 10, no. 17, p. 3195, 2022.

[6] S. Kobayashi, A. Hizukuri, and R. Nakayama, "Video anomaly detection using encoder-decoder networks with video vision transformer and channel attention blocks," pp. 1–4, July 2023.

[7] P. Khan, Y. Byun, and N. Park, "A data verification system for cctv surveillance cameras using blockchain technology in smart cities," *Electronics*, vol. 9, no. 3, p. 484, 2020.

[8] A. Chattopadhay, A. Sarkar, P. Howlader, and V. N. Balasubramanian, "Grad-cam++: Generalized gradient-based visual explanations for deep convolutional networks," *2018 IEEE Winter Conference on Applications of Computer Vision (WACV)*, pp. 839–847.

[9] R. R. Selvaraju, M. Cogswell, A. Das, R. Vedantam, D. Parikh, and D. Batra, "Grad-cam: Visual explanations from deep networks via gradient-based localization," *Proceedings of the IEEE international conference on computer vision*, pp. 618–626, 2017.

[10] R. R. Selvaraju, A. Das, R. Vedantam, M. Cogswell, D. Parikh, and D. Batra, "Grad-cam: Why did you say that?," 2017.

[11] J. An and S. Cho, "Variational autoencoder based anomaly detection using reconstruction probability.," *Special lecture on IE*, vol. 2, no. 1, pp. 1–18, 2015.