**BCSE497J - Project-I**

**REAL LIFE VIOLENCE DETECTION USING VIDEO DATASET**

**21BCE0818  TANYA BATRA**

**21BCE3826  JHA ADITYA SUBHASH CHANDRA**

**21BCE0545  ARYAN KHATUWALA**

Under the Supervision of

|  |
| --- |
| **Dr. MANOOV R**  **Assistant Professor Senior**  **School of Computer Science and Engineering (SCOPE)** |

**B.Tech.**

*in*

**Computer Science and Engineering**

**School of Computer Science and Engineering**

**A logo for a university

Description automatically generated**

November 2024

**ABSTRACT**

Real-time physical violence detection in video clip streams is a vital element of public security, monitoring as well as police. Typical security systems count on human monitoring, which leans to hold-ups and also mistakes specifically when checking big quantities of video over prolonged durations. This job resolves these constraints by suggesting a deep learning-based system that instantly spots fierce habits in real-time video clip streams. By leveraging a mix of Convolutional Neural Networks (CNNs) for spatial function removal, Long Short-Term Memory (LSTM) networks for temporal evaluation, plus MobileNetV2 for source performance the system can run successfully on low-end gadgets such as mobile phones or fundamental CCTV electronic cameras making it scalable and also sensible for real-world applications.

The job starts with information collection as well as preprocessing making use of openly offered video clip datasets having both terrible as well as non-violent activities. The information will certainly be stabilized, resized, plus raised to guarantee the version's strength in dealing with differing video clip resolutions, illumination problems, together with video camera angles. A CNN design will certainly be made to record spatial attributes in each video clip structure, adhered to by the assimilation of an LSTM network to examine the temporal dependences throughout series of frameworks. The incorporation of MobileNetV2 guarantees that the version stays computationally light-weight, permitting it to operate effectively on tools with restricted handling power.

The incorporated CNN-LSTM version will certainly be educated utilizing stratified information, with examination metrics such as precision, precision, recall coupled with F1-score leading the efficiency evaluation. Complying with effective training the system will certainly be released on side gadgets plus checked in real-time situations, such as public security video footage to assess its efficiency in finding fierce activities under real life problems. The system's capability to keep real-time efficiency with marginal latency also in resource-constrained atmospheres, will certainly be a key emphasis.

Inevitably, this job intends to develop a durable, reliable plus scalable remedy for real-time physical violence discovery in video clip streams. By incorporating innovative deep understanding methods with enhanced design styles the system looks to boost public safety and security by offering an automated, dependable coupled with exact choice to conventional security systems. The release of this modern technology can change exactly how physical violence is found as well as replied to in numerous public areas from roads and also institutions to airport terminals coupled with various other high-traffic locations, therefore adding to a much safer as well as much more safe and secure setting.

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| **Sl.No** | **Contents** | **Page No.** |
|  | **Abstract** | **2** |
| **1.** | **INTRODUCTION <Uppercase, Bold>** | **4** |
|  | 1.1 Background <Capitalize Each Word, Normal> | **4** |
|  | 1.2 Motivations | **5** |
|  | 1.3 Scope of the Project | **5** |
| **2.** | **PROJECT DESCRIPTION AND GOALS** | **7** |
|  | 2.1 Literature Review | **7** |
|  | 2.2 Research Gap | **8** |
|  | 2.3 Objectives | **8** |
|  | 2.4 Problem Statement | **9** |
|  | 2.5 Project Plan | **9** |
| **3.** | **TECHNICAL SPECIFICATION** | **11** |
|  | 3.1 Requirements | **11** |
|  | 3.1.1 Functional | **11** |
|  | 3.1.2 Non-Functional | **11** |
|  | 3.2 Feasibility Study | **12** |
|  | 3.2.1 Technical Feasibility | **12** |
|  | 3.2.2 Economic Feasibility | **13** |
|  | 3.2.2 Social Feasibility | **15** |
|  | 3.3 System Specification | **16** |
|  | 3.3.1 Hardware Specification | **17** |
|  | 3.3.2 Software Specification | **17** |
| **4.** | **DESIGN APPROACH AND DETAILS** | **19** |
|  | 4.1 System Architecture | **19** |
|  | 4.2 Design | **20** |
|  | 4.2.1 Data Flow Diagram | **20** |
|  | 4.2.2 Use Case Diagram | **21** |
|  | 4.2.3 Class Diagram | **22** |
|  | 4.2.4 Sequence Diagram | **23** |
| **5.** | **REFERENCES** | **24** |

**1. INTRODUCTION**

The real-time violence detection is an evolving and demanding domain in the area of artificial intelligence as well as public security. Given the current escalation of insecurity in many environments such as commercial places, transport systems, educational systems and monitoring systems, people turned to automated detection of violence in these surroundings. One of the major drawbacks of existing surveillance systems is that they require substantial reliance on human patrols, which causes the systems to have lapses, excessive response time, and inefficiency in resource utilization. Manually looking for violence in video streams is time-consuming and is often misinterpreted especially with too much footage available.

To deal with the shortcomings outlined above, this project comes up with a system that uses deep learning to detect violent behaviour from video datasets in real time. This system uses modern neural networks, in particular CNNs and LSTMs, to process a video stream’s spatial and temporal aspects. CNNs have great abilities of catching spatial properties inside the video frames whereas LSTMs can track time dependencies between the frames, which is very important in abuse detection. Furthermore, the MobileNet framework is assimilated in the system architecture to provide a level of speed and functionality in edge devices (smartphone, raspberry pi, etc.) Therefore, practicality and scalability is envisaged at the end for any fieldwork implementation.

This integration of deep learning and edge computing aims to overcome the limitations of current surveillance systems, providing an automated, real-time solution that enhances public safety by delivering high accuracy and rapid response in detecting violence.

**1.1 Background**

Surveillance cameras are omnipresent in modern public and private spaces, from government buildings to public parks and shopping centers. Despite their widespread usage, the effectiveness of these surveillance systems is often hampered by the sheer volume of data that requires manual monitoring by human operators. This manual observation process is not only labor-intensive but also susceptible to fatigue, distraction, and errors.

Moreover, in many surveillance scenarios, violent incidents occur suddenly and often last only for a short duration, making it difficult for human observers to detect and respond in real-time. The traditional reliance on human surveillance leads to delayed reactions, which could hinder timely interventions in preventing or mitigating violent incidents. For instance, in large-scale public spaces or during mass events, monitoring and identifying specific instances of violence in a timely manner becomes exceedingly challenging without automated assistance.

During the last couple of years, machine learning and deep learning have experienced tremendous leaps in streamlining jobs like recognizing images and videos. Using CNN and LSTM models, researchers can now construct systems that analyze both spatial and temporal data and can thus detect exact actions in video streams. Such development allows for the construction of systems that can detect violence, recognizing patterns of violent conduct and automatically notifying concerned authorities, highly improving the surveillance system. CNNs proved to be optimal in the treatment of visual data-could extricate relevant features from images while LSTMs had been used to capture temporal dependencies between consecutive frames in video data and therefore to recognize violent sequences in time.

However, with the emergence of edge computing and recent lightweight architectures in models like MobileNet, those complex deep learning models have already found their way into resource-constrained devices. This is important for real-world applications of surveillance systems to be implemented on low-end devices such as a CCTV camera, a smartphone, or a Raspberry Pi with fewer computational resources. An efficient, real-time violence detection system optimized for such devices can come to revolutionize public safety by providing scalable, low-cost solutions for automated surveillance.

**1.2 Motivations**

The real reason behind this project is public safety improvement, as an inventor introduces an automated reliable and efficient violence-detecting system in real time; conventional surveillance systems fail to suffice simply because they rely on human observers, who may miss the critical events owing to tiredness, distraction, or just because of sheer volumes of data they must monitor. The ultimate importance of building an automated system, which could immediately identify violent instances in video feeds and alert the right authorities, is to prevent escalation and improve response times in violent situations.

A further important motivation is the growing demand for a system that can work well on low-resource devices: in many settings, such as small businesses, schools, or even personal surveillance setups, there is rather limited access to high-end infrastructure capable of running complex machine learning models. The integration of MobileNet into the model architecture is in place to ensure that the system could work on edge devices with minimal computational resources to be available and deployable in a wide range of environments.

Finally, the project is motivated by a need for creating a scalable and adaptive solution that can be able to handle varied real-world scenarios. Violence comes in different forms and settings, both from well-lit, high-resolution footage in a controlled setting to low-resolution, grainy surveillance footage captured from a camera at a distance. The model should be able to handle all such variations with maximum accuracy and precision toward identifying violent behavior. Optimizing real-time performance and adding advanced deep learning techniques are aimed at creating a system that could not only detect violence but do so with minimal false positives or negatives, ensuring reliable performance in practical applications.

**1.3 Scope of the Project**The scope of this project encompasses the development of a deep learning-based system capable of detecting violent actions in real time through video feeds. The main focus of the project is in defining and selecting the proper model architecture of CNN and LSTM models for extracting both spatial and temporal information from video data. CNNs will be utilized to extract features of each frame of the video, which is related to the violence whereas features of temporal dependencies will be extracted by LSTMs for detecting sequential violent actions from the frames of the video. The proposed CNN-LSTM model is to be enhanced for lightweighting by deploying MobileNetV2; a small CNN network that is suitable for low-powered IoT end devices.

The system will be trained on other public databases that come with labelled examples of violent and non-violent actions. After training of the model, it will be used to test in the actual surveillance environment, and determine its performance in distinguishing between violence in a correct and faster manner. Further, the task will also be based on fine-tuning the model for operation on low-end devices such as smartphones and Raspberry Pi. This entails the reduction of computation and the amount of memory that is used in order to enable the work of the model to be done in real-time with less delay.

**2. PROJECT DESCRIPTION AND GOALS**

The objective of this project is therefore to design and build an end to end deep learning based system for real time identification of persons engaging in violent conduct in a video stream. The system proposed will involve incorporation of CNNs to analyze spatial mapping of each frame of the video and LSTM to analyze temporal interactions of frames. The MobileNetV2 model that is a lightweight neural network model will be integrated to the system to ensure that it can run on edge devices such as smartphones, CCTV cameras and other low resource devices.

The final application of the project is to implement this system in a live environment where this system would be further modified and fine tuned to produce proper results. In an effort to enhance current surveillance systems the project aims at applying modern machine learning techniques to the problem of violence recognition in real-time with high accuracy given the current challenges of limited resources for such systems.

**2.1 Literature Review**

Indeed the area of detection of violence has received major strides especially over the last few years because of the developments made in machine learning and deep learning algorithms. However, the majority of works has been conducted using artificially generated datasets which are far from the real-world scenarios of surveillance contexts. Previous techniques for violence identification included the conventional machine learning techniques, for instance, SVM, or Random Forests, or Decision Trees. While these models where sensible the approach used was not capable of providing real time results and at the same time some additional features where manually included. Furthermore, they failed in the aspect of versatility that is extremely important for the large scale, and multifaceted settings.

Some of the most recent models include CNNs and these have given very good performances especially in real tasks such as image or video recognition. CNNs are more suited for recognising spatial patterns and are therefore preferable for identifying particular violent actions in individual frames of video. At the same time, LSTMs, which are developed to analyze temporal relations in the sequential data, work well within the video sequences and in analyzing actions taking place during the shooting.

Another significant improvement regarding the detection of violence is the use of compact neural network architectures such as MobileNetV2. MobileNetV2 is optimized for speed execution on devices such as mobile which are resource limited in terms of processing power and memory. This makes it a primary piece of equipment in creating structures that must function in real-time on a low resource apparatus, for instance, mobile or inexpensive CCTV systems.

However, there are still some gaps that the current literature and systems contain and this project will contribute to fill those gaps. Thus, the objective has been set to achieve a novel model for increasing the power of hyperparameter-tuning on the basis of the CNNs, LSTMs, and the MobileNetV2 to create a lightweight, real-time system even for the environment, in which such power is limited.

**2.2 Gaps Identified**

Several gaps in the existing research and violence detection systems have been identified:Several gaps in the existing research and violence detection systems have been identified:

Lack of Support for Low-End Devices: Most of the violence detection systems are developed to run on sophisticated hardware which comes with huge computational power. A special emphasis here is felt concerning models that can be run on low-end hardware as, for instance, smartphone or basic CCTV systems which are a typical case in real-world scenarios.

Artificial Datasets: Most of the current models are initiated with synthetic data sets that tend to differ from the real video feed capabilities. Some real-world footage constraint could be low video quality, noisy video, unclear video, and orientation or angle used when creating the footage all of which can greatly affect the model.

Real-Time Performance: A non-trivial number of deep learning-based systems are not designed for real-time operation. This is especially so in situations where there cannot be any delay in identification of such incidents and a quick and appropriate response, for instance in violent occurrences. While high accuracy is generally desirable, it is not unusual for such systems to have high latency— this can greatly reduce the applications’ utility in real life situations.

Lack of Integrated Systems: The CNN are effective in recognizing spatial features while the LSTMs are most efficient in temporal analysis, but the integration of both the approaches has not been well implemented in the existing systems for developing a perfect violence detection model. It is therefore important to note that majority of them design algorithms for either spatial or temporal features but not both thus they may lack accuracy as well as reliability.

**2.3 Objectives**

The project has several key objectives:

CNN for Spatial Feature Extraction: The system will use CNNs to extract spatial features from each frame of the video since the videos are short and contain only one action. This will enable the system to consider violent action that can be recognized from visual Information in two consecutive frames like the motion or the position of the limbs.

LSTM for Temporal Analysis: This feature will be achieved by using LSTM networks for identification of temporal relations between the frames enabling one to detect violent actions that are preceded over several frames. This will enhance the capacity of the system to capture events that happen over a period; like fighting or assaulting.

It is mandatory to achieve high optimization for the system for it to run efficiently on edge devices. In order to attain that in this project, the MobileNetV2, lightweight neural network architecture will be utilized since they can run well in resource constrained environments. I will have to ensure that I have optimized the model to run on these devices especially the smartphones or raspberry pi systems while at the same time maintaining a real time performance.

Training and Evaluation: The integrated CNN-LSTM model will be trained on a labeled dataset of violent and non-violent action. This will afford greater measure of reliability of the system to detect violence and its outcomes such as accuracy, Precision, and Recall.

Real-Time Deployment: The last step is to test the model in real life through real time video feeds of surveillance cameras to be worked on. The performance of the system will be measured in terms of accuracy, latency, and computational time with a specially designing goal to achieve robustness to different settings of environment such as video, light, and camera perspective.

**2.4 Problem Statement**

There are so many limitations confronting the current surveillance systems particularly when it comes to tracking violence. Observation and assessment of large amounts of video material by persons is a highly time-consuming, inaccurate, and imprecise process. Furthermore, existing automatic systems involve a high level of hardware dependency as well as artificially engineered datasets. These systems usually do not have the feature of functionality in such constrained capacities as low end CCTV systems or mobile applications. Further, they do not provide real-time results as needed when violence is being acted out in any of its forms.

The issue that is addressed by this project is the absence of an automatic, reliable, and effective system that can analyze video streams to estimate the tendency towards violence in real time. The system must also be able to perform well on low end devices and on limited processing power, and on videos with bad capture, low quality and inconsistent lighting, and shot from various angles.

**2.5 Project Plan**

The project will be executed in several phases to ensure a systematic approach to development and deployment:he project will be executed in several phases to ensure a systematic approach to development and deployment:

Data Collection and Preprocessing: The first phase includes gathering a large amount of data of violent and non-violent behaviors from the open-source video databases. This dataset will incorporate a vast number of real-life cases and a variety of lighting condition, angles, and video resolution. Prior processing steps of normalization and resizing of frames will be implemented in addition to data augmentation to improve the models resilience. Data augmentation will also play an important role for creating more realistic environment by adding noise, changing illumination, and rotating frames with respect to various orientations of camera.

Model Design: In this phase, there will be a CNN model whose role will be to find spatial features from each video frame being received. The CNN will be designated to recognize signs connected with performative aspect of violence, like rapid body movements and aggressive positioning of limbs. An LSTM network will then be incorporated into the system to identify time dependencies of frames so that the system can detect sequences of violence.

Optimization with MobileNetV2: MobileNetV2 will be considered to add to the model architecture that would make it possible for it to work on low-end devices. This will entail finding ways in which the above aspects can be enhanced even further in terms of computational efficiency with respect to the number of computations and memory foot print of the model while at the same time improving the accuracy and real-time performance of the model.

Training and Evaluation: Thereafter, the training process of the combined CNN-LSTM model will involve cross validation and/or hyper parameter tunning of the preprocessed dataset. Various measures including, accuracy, precision, recall and F1 score will be used to assess the performance of the model. The high accuracy and speed of the system should be high, with the least number of false positives while at the same time avoiding high false negatives in that it should be able to detect violence.

Real-Time Deployment and Testing: After that model has been trained and tested, it will be used in a low power device like Raspberry Pi portable computer. The true potential of the system in terms of real-time data processing will be demonstrated using experiment examples of actual surveillance, for instance, CCTV video streams coming from various public areas. The aim is to evaluate the performance of the system under real-life conditions with particular reference to cameras with lower resolution, changing lighting environments and multiple view points.

Final Evaluation and Feedback: Once the system has been implemented, there will be changes which will be incorporated into it since the performance of the system when it is out in the field is always different from the performance of the system when it is still in the developmental stage. Further, the feedback from the users will be considered to enhance the overall efficiency, accuracy as well the usability of the system. For future enhancements, there is a possibility of using more than one data feed which can include audio feed so as to increase the probability of detections as well as improving the efficiency of the real-time detection that the system is expected to perform on the edge devices.

**3. TECHNICAL SPECIFICATION**

**3.1 Requirements**

***3.1.1    Functional***

1. **Input Video Feed (Dataset):** The system must be able to accept real-time video feeds from cameras or prerecorded video datasets.
2. **Frame Extraction:** Extract video frames at regular intervals for processing.
3. **Preprocessing:**

* Resize, normalize, and augment video frames to match MobileNet's input specifications.
* Convert video frames into sequences suitable for LSTM processing.

1. **Violence Detection:**

* Utilize the MobileNet architecture for feature extraction from each frame.
* Use CNN to learn spatial patterns and features related to violence.
* Feed extracted features into an LSTM layer to analyze temporal sequences and detect potential violence over time.

1. **Real-time Prediction:**

* Generate predictions in real-time and classify sequences as "violent" or "non-violent."

1. **Alert System:** Trigger an alert (e.g., email, sound, or notification) when violence is detected.
2. **Accuracy Metrics:** Display accuracy, precision, recall, and F1-score of the model after training.
3. **Logging and Reporting:** Maintain logs for detected events, timestamps, and other relevant metadata.
4. **Scalability:** Ability to handle multiple video feeds concurrently.
5. **Continuous Learning:** Ability to update the model with new datasets to improve detection performance over time.

**3.1.2 Non-Functional**

1. **Performance**:

* The system must process frames at a minimum of 30 frames per second to ensure real-time analysis.
* Latency between the event happening and alert generation should be minimal (less than 1 second).

1. **Scalability**:

* The architecture must support scaling to handle higher volumes of video streams without degradation in performance.

1. **Accuracy**:

* The model should maintain a high detection accuracy (e.g., >90%) in diverse environments and lighting conditions.

1. **Robustness**:

* The system should work effectively in various scenarios such as crowded environments or partial occlusions.

1. **Resource Efficiency**:

* MobileNet should be used to ensure the system is computationally lightweight and can run on edge devices with limited resources.
* Optimize GPU/CPU usage for real-time processing without overloading the system.

1. **Security**: Ensure secure access to video streams and store event logs securely to prevent tampering.
2. **Usability**:

* The system must have an intuitive interface for configuring the video feed, setting detection thresholds, and managing alerts.

1. **Maintainability**: The system should be easy to update, debug, and maintain with modular components for easy troubleshooting.
2. **Resilience**: System should handle network or hardware failures gracefully, retrying connections or alerting operators if feeds go down.

**3.2 Feasibility Study**

**3.2.1 Technical Feasibility**

1. **Technologies Used**:
   * **MobileNet**: This lightweight, efficient neural network architecture is well-suited for real-time feature extraction from video frames. It is optimized for low-latency applications and can run on edge devices (e.g., smartphones, embedded systems) or on cloud-based servers with limited resources. The pre-trained models of MobileNet can significantly reduce development time by leveraging transfer learning.
   * **CNN (Convolutional Neural Networks)**: CNNs are ideal for spatial feature extraction, which is critical for detecting visual patterns related to violence, such as sudden movements or specific actions. CNNs can be efficiently implemented with GPU acceleration, and their integration with MobileNet ensures that computational overhead is kept to a minimum.
   * **LSTM (Long Short-Term Memory)**: LSTMs are crucial for temporal sequence analysis, as they can capture motion patterns over time. LSTMs work effectively when paired with CNNs for video data, allowing the system to track events and detect violence in sequences rather than just individual frames. Existing libraries like TensorFlow and PyTorch provide robust support for LSTM models.
   * **Real-time Processing Frameworks**: OpenCV or other video processing libraries can be used for frame extraction and manipulation, ensuring that frames are preprocessed efficiently for input into the MobileNet-CNN-LSTM pipeline. These libraries have support for real-time video handling, making them highly suitable for the task.
2. **Infrastructure and Hardware Requirements**:
   * The system can be implemented on various hardware platforms depending on the use case:
     + **Edge Devices**: For lightweight deployments, the system can run on edge devices with moderate processing power (e.g., Nvidia Jetson, smartphones) using optimized models.
     + **Cloud/Server-based Processing**: For environments where more significant computational power is available, the system can scale using cloud infrastructure or dedicated GPUs to handle multiple video streams simultaneously. Platforms like AWS, GCP, or Azure can offer scalable infrastructure.
     + **GPU Utilization**: To achieve real-time processing, GPU acceleration is recommended for handling the CNN and LSTM model layers, reducing frame processing time and ensuring the system meets performance benchmarks.
3. **Software and Tools Availability**:
   * **Deep Learning Frameworks**: Popular frameworks such as TensorFlow, Keras, and PyTorch are readily available and provide support for MobileNet, CNNs, and LSTM models. These libraries include pre-trained models, saving development time.
   * **Video Processing**: Open-source libraries like OpenCV offer extensive support for real-time video feed handling, frame extraction, and manipulation, allowing for easy integration with the deep learning model pipeline.
   * **Deployment Tools**: Tools for deployment, such as Docker for containerization and Kubernetes for scalability, are available for managing real-time video streams across multiple instances. These tools ensure that the system can be efficiently deployed in a variety of environments.
4. **Development Resources and Expertise**:
   * The required expertise to implement the system (deep learning, video processing, software engineering) is widely available. The availability of online tutorials, open-source resources, and pre-trained models accelerates the development process. Developers familiar with deep learning architectures, real-time processing frameworks, and cloud deployment can easily build and scale the system.
5. **Risks and Mitigation**:
   * **Computational Complexity**: The combination of MobileNet, CNN, and LSTM introduces some computational complexity, but using pre-trained models and optimized frameworks like TensorFlow Lite or ONNX can mitigate this issue.
   * **Latency Challenges**: Processing video in real-time may introduce latency, especially in high-resolution or crowded environments. Optimization techniques, such as frame sampling or running models on GPUs, will be necessary to meet real-time performance targets.
   * **Model Accuracy**: Achieving high accuracy in diverse environments (e.g., varying lighting conditions, occlusions) could be challenging. Continuous model training and using large, diverse datasets will help improve the robustness of the model.

**3.2.2 Economic Feasibility**

1. **Initial Development Costs**:

* **Software Development**: The primary cost will be the development effort, including building the violence detection system using MobileNet, CNN, and LSTM. This involves coding, testing, and integrating components like video processing, model training, and alerting systems. Depending on the team's expertise, this can be done in-house or outsourced.
* **Pre-trained Models**: Using pre-trained MobileNet and CNN models reduces both time and cost significantly, as training from scratch would be computationally expensive. Many pre-trained models are freely available under open-source licenses.
* **Frameworks and Libraries**: Most deep learning libraries (e.g., TensorFlow, PyTorch, Keras) and video processing tools (e.g., OpenCV) are open-source and free to use, minimizing software costs.
* **Hardware**: Initial hardware setup depends on the system’s deployment environment:
  + **Edge Devices**: In smaller-scale implementations (e.g., a single camera), affordable devices like Nvidia Jetson ($100-$500) or Raspberry Pi ($35-$100) can be used.
  + **Server or Cloud-based Processing**: For larger setups, investment in server-grade hardware (GPUs) or cloud infrastructure (AWS, GCP, Azure) is required. Cloud services can start at minimal costs (e.g., $100/month for moderate usage) and scale based on demand.
* **Data Collection and Labeling**: If a custom dataset is required for training and validation, additional costs may arise from curating and labeling video datasets. However, many public datasets are available for violence detection tasks, minimizing this expense.

1. **Operational Costs**:

* **Cloud Infrastructure**: Ongoing cloud service costs will depend on the number of video streams processed and the computational requirements of the models. Cloud providers offer flexible pricing, ranging from a few hundred dollars per month for small setups to several thousand dollars for large-scale operations.
* **Hardware Maintenance**: For edge devices or server setups, periodic hardware maintenance and replacement (e.g., GPUs, cameras) will incur ongoing costs. The frequency of this will depend on the deployment environment and the hardware's longevity.
* **Electricity Costs**: Both server-grade and edge devices will require continuous power, contributing to operational costs, especially for larger installations with multiple cameras.

1. **Cost-Benefit Analysis**:

* **Cost Savings**:
  + **Automation**: By automating violence detection, the system reduces the need for human monitoring, saving on personnel costs for security teams. This is especially beneficial in environments with 24/7 monitoring requirements.
  + **Prevention of Damages**: Timely detection of violent incidents can help prevent escalations, reducing potential damages to property, legal costs, and liability for organizations.
  + **Public Safety**: Enhancing security and preventing violence may improve the overall safety of the community, potentially reducing insurance premiums for some businesses and increasing their value proposition.
* **Revenue Generation**: For companies deploying this technology (e.g., security firms or SaaS providers), the system can be marketed as a product, generating revenue from clients needing advanced video analytics.
* **Long-Term Cost Reduction**: The system will benefit from continuous improvement, where retraining and fine-tuning models with new data enhance accuracy. As hardware becomes more affordable, future expansions will be more economical.

1. **Training and Personnel Costs**:

* **Employee Training**: Personnel responsible for managing the system (e.g., IT staff) will need training to understand model deployment, configuration, and alert management. This can be done internally or through third-party resources, with minimal costs.
* **Support and Maintenance**: Ongoing technical support for maintaining the system (e.g., updating models, handling bugs) will require dedicated personnel, either full-time or on a contracted basis. In-house IT staff can cover much of this, especially in small-scale deployments.

1. **Return on Investment (ROI)**:

* **Short-Term ROI**: While initial investment in development and deployment might be significant, the system can offer immediate returns in terms of improved security and reduced human labor costs.
* **Long-Term ROI**: Over time, operational costs will stabilize, and the system’s accuracy will improve with more training data. This allows businesses to scale without a proportional increase in costs. Savings from automated monitoring, improved safety, and prevention of incidents contribute to a strong long-term ROI.

1. **Alternatives and Cost Comparisons**:

* **Human Surveillance**: Continuous human surveillance is costly and prone to fatigue or oversight. Real-time violence detection can be a more reliable and cost-efficient solution, especially when scaling to multiple camera feeds.
* **Off-the-Shelf Solutions**: While off-the-shelf violence detection systems exist, they are often expensive and lack customization options. Building an in-house solution allows for more tailored functionality and long-term cost savings.

**3.2.3 Social Feasibility**

1. **Public Safety and Security**:

* The primary social benefit of the system is the enhancement of public safety. By enabling real-time detection of violent events, the system can help law enforcement and security personnel respond more quickly to incidents, potentially preventing escalation and reducing harm to individuals.
* The presence of such a system in public spaces like schools, transportation hubs, or public events can provide a sense of security and confidence for the community. People are likely to feel safer knowing that advanced technology is being used to protect them.

1. **Reduction in Crime**:

* Early detection and prevention of violent incidents can contribute to a reduction in crime rates. The system acts as both a deterrent for potential offenders (due to the higher likelihood of detection) and an effective response mechanism for law enforcement.
* In high-risk areas, this can lead to improved social order and trust in security measures, fostering a more stable environment.

1. **Ethical Concerns and Privacy Issues**:

* **Surveillance Concerns**: One of the main social challenges with real-time violence detection systems is the potential for privacy invasion. Constant video surveillance, even when focused on detecting violent behavior, may raise concerns about the extent to which individuals are being monitored.
* **Data Privacy**: There may be public concern over how video data is stored, who has access to it, and how long it is retained. This requires the system to adhere to strict data privacy laws and ensure that data is anonymized when necessary and protected from unauthorized access.
* **Transparency**: The system should be implemented with clear communication to the public regarding its purpose, limitations, and how the collected data will be used. Transparency in these aspects will help mitigate privacy concerns and build trust.

1. **Community Acceptance**:

* **Positive Reception**: In environments where security is a priority (e.g., schools, airports, public transportation), the community is likely to accept and support the system as an additional layer of protection. People generally view such technology as a proactive measure to safeguard public spaces.
* **Stakeholder Buy-In**: Gaining the support of key stakeholders (e.g., law enforcement, local governments, private organizations) is crucial. Demonstrating the system's ability to prevent violence, reduce crime rates, and provide reliable security may help secure stakeholder investment and community approval.
* **Social Stigma**: There may be concerns about how the system might disproportionately monitor certain groups or neighborhoods. Addressing these concerns through equal implementation and sensitivity to ethical deployment will be necessary to avoid social stigmatization.

1. **Impact on Employment**:

* **Complementing Human Security**: The system will complement, rather than replace, human security efforts. While it reduces the need for continuous human surveillance, it will still require human operators to manage the system, respond to alerts, and interpret events flagged as violent. This ensures that jobs in security services are not entirely displaced but enhanced through technology.
* **New Opportunities**: The adoption of this technology can lead to the creation of new roles in areas such as system maintenance, data analysis, and software support. It may also create opportunities for retraining current security personnel to work alongside the system effectively.

1. **Public Trust and Legal Compliance**:

* **Regulatory Framework**: Compliance with local laws and regulations regarding surveillance and data protection is essential. Aligning the system with regulations such as the General Data Protection Regulation (GDPR) or other regional data privacy laws ensures that the system is legally acceptable and increases public trust.
* **Public Awareness Campaigns**: To ensure social feasibility, public awareness campaigns that explain the benefits, limitations, and privacy protections of the system should be implemented. These campaigns can help build trust and ensure the community understands the system's role in violence prevention.

**3.2 System Specification**

**3.2.1 Hardware Specification**

1. **Edge Devices** (For lightweight, local processing):
   * **Device**: Nvidia Jetson Nano / Nvidia Jetson Xavier / Raspberry Pi 4  
     These devices are suitable for small-scale, real-time video processing with the MobileNet, CNN, and LSTM models.
   * **Processor**: Quad-core ARM Cortex-A57 (for Jetson Nano) or Hexa-core ARM v8.2 (for Jetson Xavier)
   * **GPU**: 128-core Nvidia Maxwell GPU (for Jetson Nano) or 512-core Volta GPU (for Jetson Xavier)
   * **RAM**: Minimum 4 GB for Jetson Nano, 8-16 GB for Jetson Xavier
   * **Storage**: 32 GB SD card for OS and application storage
   * **Power Supply**: 5V 4A for Jetson Nano / 19V 3.42A for Jetson Xavier
   * **Camera**: High-definition IP camera with minimum 720p resolution, 30 FPS for video capture
2. **Server/Cloud-Based Deployment** (For large-scale or distributed environments):
   * **Processor**: Multi-core Intel Xeon or AMD EPYC (minimum 8 cores)
   * **GPU**: Nvidia Tesla T4, V100, or A100 (depending on the number of video streams and computational requirements)
   * **RAM**: Minimum 32 GB for server-based processing
   * **Storage**: SSD-based storage with at least 512 GB capacity, scalable depending on the amount of video data and model storage
   * **Network**: High-speed Ethernet or fiber optic connection for real-time video streaming and processing
   * **Camera**: High-resolution IP cameras (1080p or higher) with night vision and motion detection capabilities for enhanced video capture
   * **Cloud Infrastructure (if applicable)**:
     + **GPU instances**: AWS EC2 P3 or G4 instances, GCP AI Platform, or Azure GPU VM Series for scalable real-time processing
3. **Network Components**:
   * **Router/Switch**: Gigabit Ethernet router for handling multiple camera streams, ensuring low-latency data transfer to processing units.
   * **Bandwidth Requirements**: Each 720p video stream requires approximately 2-5 Mbps, while 1080p streams require 5-10 Mbps. For multiple cameras, sufficient bandwidth must be provisioned to avoid bottlenecks.
   * **Latency Consideration**: The network should have minimal latency to ensure real-time video transmission to processing units.
4. **Power Supply**:
   * **Uninterruptible Power Supply (UPS)**: To ensure continuous operation, particularly in critical environments like security surveillance. A UPS with at least 500VA rating is recommended to handle brief power outages and protect equipment.
   * **Edge Devices**: Portable power solutions or battery backup in case of power loss, especially for edge deployments in remote areas.

**3.2.2 Software Specification**

1. **Operating System**:
   * **Edge Devices**: Ubuntu or JetPack SDK (Nvidia Jetson), Raspberry Pi OS.
   * **Servers/Cloud**: Ubuntu Server, AWS, GCP, or Azure environments.
2. **Deep Learning Frameworks**:
   * **TensorFlow/Keras**: For MobileNet and LSTM-based model development.
   * **PyTorch**: Optional alternative for model training.
3. **Computer Vision Libraries**:
   * **OpenCV**: For video processing and frame extraction.
   * **FFmpeg**: For handling various video formats.
4. **Pre-trained Models**:
   * **MobileNet**: For feature extraction from video frames.
   * **LSTM**: For analyzing temporal sequences.
5. **Model Training Tools**:
   * **Google Colab / Jupyter Notebooks**: For model development.
   * **TensorBoard**: For visualizing training performance.
6. **Backend Server**:
   * **Flask** or **FastAPI**: For deploying the violence detection model via APIs.
   * **Gunicorn**/**Uvicorn**: For managing production environments.
7. **Database** (optional):
   * **MongoDB/PostgreSQL**: For logging incidents and metadata storage.
8. **Real-time Processing**:
   * **Kafka/RabbitMQ**: For managing real-time video streams.
   * **Twilio/SendGrid**: For notifications when violence is detected.
9. **Cloud Integration**:
   * **AWS Lambda**/**Google Cloud Functions**: For serverless deployment.
   * **S3 Buckets/Google Cloud Storage**: For video and data storage.
10. **Security**:

* **OAuth 2.0**/**SSL/TLS**: For secure authentication and data encryption.

1. **Development Tools**:

* **VS Code/PyCharm**: IDEs for development.
* **Git/GitHub**: For version control.

**4.DESIGN APPROACH AND DETAILS**

**4.1 System Architecture:**

The architecture diagram outlines a Violence Detection System based upon video capture and ML algorithms. This section sheds light on the parts of the above mentioned systems and their cooperative work:

User – A person who interacts with the system through a dashboard for viewing detection results and modification of parameters.

Input (Camera/Video Streams) - This is an area of the system where cameras are connected to capture live or recorded videos which is the major input in the system.

Preprocessing:

Frame Extractor: It works to access and retrieve images or individual frames from the video clips for image scrutiny.

Data Cleaner: Cleaning the images obtained from frame extraction (i.e. noise removal) to increase the chances of detection.

Model: a violence detection model which may based on machine learning or deep learning techniques such as CNN, RNN is used to analyze the preprocessed frames to classify if a violent action takes place or not.

Postprocessing:

Alert System: If violence is detected, instant warnings for example SMS, Warnings, or emails are generated.

Logging Service – This system captures the details of the detection events such as how long they last, where they happened and even video images or clips if available into the databases for record purposes.

Storage:

Database: Stores logs and detection details.

Video Storage: Archives the video streams or important video clips related to detected incidents.

User Interface (Dashboard/Alert Viewer): Allows the user to view alerts, logs, and interact with the system to manage settings and view reports.

Data Flow:

Camera/Video Streams → Frame extraction → Data cleaning → Violence Detection Model → Alerts or Logs

Alerts and logs are stored and can be accessed by users via the Dashboard.

In summary, the system takes in video feeds, preprocesses them, runs a violence detection model, and triggers alerts or stores logs for user interaction via a user interface.

**A diagram of a computer

Description automatically generated**

**4.2 Design**

***4.2.1  DATA FLOW DIAGRAM***

**A screenshot of a computer flowchart

Description automatically generated**

***4.2.2  Use case diagram:***

***A diagram of a crime investigation system

Description automatically generated***

***4.2.3  Sequence diagram***

***A diagram of a diagram

Description automatically generated***

**5. REFERENCES**

**Weblinks:**

[**https://www.kaggle.com/datasets**](https://www.kaggle.com/datasets)

[**https://www.geeksforgeeks.org/machine-learning-model-evaluation**](https://www.geeksforgeeks.org/machine-learning-model-evaluation/)

**Journals:**

**Conference:**

**Book:**