**Key words**

**zero-knowledge encryption**

Video surveillance systems have evolved from traditional recording methods to more advanced, automated solutions aimed at enhancing security and crime prevention. These systems face challenges in storage capacity, human monitoring resources, and effective object detection (M. V. Khadse et al., 2016). Smart video surveillance incorporates automated functions for object detection, identification, and tracking, though these capabilities are still limited (S. Abdurrahman, 2016). The complexity of modern surveillance systems introduces cybersecurity risks, including threats to hardware, firmware, and network communications (Andrei Costin, 2016). Research efforts focus on improving crime activity recognition through various techniques, such as facial expression recognition and alert systems (Kishore Kumar Kamarajugadda & H. Reddy, 2022). Despite advancements, challenges persist in areas like object identification, recognition, and tracking (S. Abdurrahman, 2016). Ongoing research aims to enhance the security, privacy, and effectiveness of video surveillance systems in crime detection and prevention.

In this assignment you will submit a 3-5 minute video presentation explaining the basic concept of your project.

This video should cover:

* The idea for the project
* Name which template you have used for the project
* Motivation for the project (why would people want this project?)
* 2-4 examples of related projects, which you should also evaluate and use to explain the motivation for the project (e.g. what is missing in these other projects)

We recommend using visual supporting elements for your presentation (e.g. powerpoint or similar slides). The video does not need to include footage of you face.

## Review Criteria

You will be marked according to the following criteria:

1. Does the report display knowledge of the area of study, previous work and academic literature?
2. Does the report critically evaluate the previous work and/or academic literature?
3. Is the project concept justified based on the domain and users?

Title: Smart Video Surveillance system limited to edge computing devices targeted at Home owners and small and medium scale organization with limited resources

# Introduction

The contribution of traditional first-generation video surveillance systems over the years has been remarkable. Before their invention, it was unimaginable to accurately replay a crime scene days after an event had occurred. The ability to capture such footage revolutionized the legal system in many countries, providing pivotal evidence that could exonerate the innocent or convict criminals beyond a reasonable doubt [1]. As noted by author [2], surveillance cameras have been widely deployed in banks, supermarkets, and parking lots, primarily serving as forensic tools to aid in post-event investigations.

Despite the strengths of traditional video surveillance systems, these systems have traditionally focused more on deterrence than on real-time prevention, as they continuously record scenes regardless of whether any significant activity is present [1]. For real-time intervention in security breaches, constant human monitoring is necessary [3]. This dependence was a consequence of technological limitations in earlier computer systems, which lacked the ability to process video information in real-time.

However, recent advancements in computer vision and artificial intelligence have transformed this landscape. Modern video surveillance systems are now capable of analyzing and interpreting video streams in real time, detecting and tracking objects, identifying abnormal activities, and generating automatic alerts without the need for constant human supervision. These developments significantly enhance real-time security, making continuous manual monitoring unnecessary.

The rise of the internet has also enabled remote surveillance, allowing users to monitor their properties from anywhere. This empowers individuals to respond swiftly to threats and de-escalate situations, even when far from their homes. However, with this increased functionality comes new cybersecurity challenges. Remote monitoring systems are vulnerable to attacks that could lead to video footage leaks or system slowdowns through Distributed Denial of Service (DDoS) attacks. These concerns pose significant privacy risks, especially in indoor settings where unauthorized access to video footage can have severe consequences.

To address these challenges, modern cryptographic techniques, such as RSA-256, AES, and zero-knowledge proof algorithms, provide robust security measures. These advancements ensure that sensitive video data can be securely transmitted and stored, safeguarding user privacy even in a connected world.

This project aims to leverage cutting-edge technologies in computer vision and cryptography to develop a video camera surveillance system using budget-friendly edge computing hardware. The system will offer advanced features such as intruder detection, alert generation, and secure remote monitoring. Designed specifically for homeowners and small-to-medium business owners, this solution will provide a balance between security, privacy, and accessibility, ensuring users can protect their properties without compromising on privacy.

Related Work

Identified problems

Proposed Solution/ Aims / Objectives

Methodologies

Conclusion

# Problems to be Solved

## ~~Efficient Review of Surveillance Footage~~

~~Problem: Users often find it impractical to review long stretches of uneventful surveillance footage. Traditional systems may record hours of footage with minimal activity, making it difficult for users to identify significant moments.~~

~~Proposed Solution: Implement video summarization techniques that condense surveillance footage into clips highlighting notable actions or events, such as intruder detection, object movements, or specific zone breaches. This feature reduces the time needed for review by focusing on the most important moments.~~

## ~~Storage Optimization for Continuous Surveillance~~

~~Problem: Home users may lack the necessary storage capacity to record continuous surveillance footage. Storing hours of footage with little or no movement wastes valuable resources.~~

~~Proposed Solution: Introduce motion-triggered recording that only saves footage when significant activity is detected. By minimizing redundant footage, this feature conserves storage space while ensuring that key events are captured.~~

## ~~Secure remote access for privacy-preserving surveillance video transmission~~

~~Problem: For home users who prioritize privacy and want to avoid third-party cloud services due to concerns about data breaches or misuse, local surveillance provides a more secure option. However, this approach often limits the ability to monitor live feeds remotely. The challenge is to develop a system that allows secure, encrypted remote access to surveillance footage while minimizing privacy risks, ensuring that sensitive video data is stored and transmitted securely.~~

~~Proposed Solution: A locally hosted surveillance system that ensures data privacy by keeping footage and metadata on-site while still allowing remote access via secure, encrypted channels. This balances the need for privacy with the convenience of remote monitoring.~~

## ~~Limited Time for Monitoring Surveillance Footage~~

~~Problem: Homeowners and SME with valuable items often seek real-time security monitoring but lack the resources to hire full-time security personnel or the time to actively watch surveillance footage. These users require a system that provides timely, automated alerts when a potential intruder is detected without requiring constant human supervision.~~

~~Proposed Solution: An intelligent surveillance system that detects motion, automatically triggers alerts, and records relevant video clips only when activity is detected, allowing users to focus on urgent threats without manual monitoring.~~

## Alerting Users Based on Prolonged Presence in Designated Critical Areas

Problem: In certain scenarios, an individual’s prolonged presence in specific critical areas may raise concerns. These concerns can arise due to reasons such as:

1. Potential discovery of hidden personal or valuable items.
2. Inability to properly operate essential equipment, leading to risks or inefficiencies.
3. Other security or operational vulnerabilities tied to extended stays in high-risk zones.

Proposed Solution: A surveillance system that monitors the duration of a person’s presence in predefined sensitive areas. If an individual remains in a critical zone (e.g., near valuable assets or high-risk equipment) beyond a set threshold, the system issues an alert. This proactive measure provides an early warning system to detect suspicious behavior or potential hazards before they escalate into more serious incidents.

Intruder Detection

Problem: Homeowners and SME with valuable items often seek real-time security and will like for a more preventive approach instead of the deterrence approach provided by traditional surveillance system. The would like to know at the very instance their space is potentially compromised by an intruder. With traditional system, this is only possible with 24/7 monitoring of the real time video footage by dedicated supervisor which is not a practical solution for home owners and small-to medium business owners as it significantly increases security cost. These users require a system that provides timely, automated alerts when a potential intruder is detected without requiring constant human supervision.

Proposed Solution: An intelligent surveillance system that detects motion, automatically triggers alerts, and records relevant video clips only when activity is detected, allowing users to focus on urgent threats without manual monitoring.

Compromised Region of interest (ROI) Detection

Problem: In certain scenarios, an individual’s prolonged presence in specific ROI may raise concerns. These concerns can arise due to reasons such as:

1. Potential discovery of hidden personal or valuable items.
2. Inability to properly operate essential equipment, leading to risks or inefficiencies.
3. Other security or operational vulnerabilities tied to extended stays in high-risk zones.

Proposed Solution: A surveillance system that monitors the duration of a person’s presence in predefined sensitive areas. If an individual remains in a ROI (e.g., near valuable assets or high-risk equipment) beyond a set threshold, the system issues an alert. This proactive measure provides an early warning system to detect suspicious behavior or potential hazards before they escalate into more serious incidents.

Compromised Item of Interest (IOI) Detection

The idea of IOI is similar to ROI but the only difference is that the movement of an item from it original and fixed location might indicate a potential theft. For instance, movement of fixed item like TV from its stand is consider a rare occurrence and can indicate theft.

Proposed Solution: A surveillance system that monitors and generate alarm when there is a movement of an IOI from its original location.

Robust Alert System

Problem: there is a chance for a user to miss the VSS alert notification if the notification are not sent to media where users are most active. Also, sometimes, a medium might be unavailable for a user depending on their location, for example, a user working offshore and out of SMS network coverage but have access to the location independent internet access might miss out on alerts if alerts are only configured to be send to mobile SMS available medium for sending notification. Thus there is need for alerts to be sent to multiple medium to improve the chance of a user missing out on notification.

Proposal solution:

1. Implement a VSS to send alerts to multiple media were users are active and used to checking. Mediums like SMS, WhatsApp and email to improve the likelihood of receiving alerts and mitigating against missing out on alerts due to loss of coverage on single media.

Event Metadata collection and Text Description of events/ occurrence in an video recording triggered by the alert system

Problem:

1. Traditional VSS alerts lack context, making it difficult to assess the urgency of an event (e.g., human vs. animal intrusion). How can integrating metadata help generate detailed, context-aware alerts to improve response accuracy and efficiency?
2. Retrieving specific events from archived VSS footage is time-consuming due to limited searchability. How can adding metadata (e.g., time, object type) streamline event searches, enabling faster evidence retrieval and supporting efficient investigations?

Solution:

Implement a system capable generating meta data such as human vs animal in motion identification, time of event, entrance direction, intrusion vs ROI vs IOI detection classification, speed of object under focus, number of intruders etc. System should be capable of associated generated metadata with saved video content.

Optimize storage and reduce review time

Problem:

Although traditional system is good as use for forensic tool for providing useful video recording evidence after the event, it does some by recording everything including uneventful with minimal and less useful activity.

1. This leads to wastage of valuable storage resources and thus drastically increase the storage requirement ad impose overhead cost on storage to the users.
2. In this situation, users also find it impractical to review long stretches of uneventful surveillance footage.

Proposed Solution:

These project retains the forensic property that traditional but deals it the storage limitation by:

1. Implement motion-triggered recording that only saves footage when significant activity is detected. By minimizing redundant footage, this feature conserves storage space while ensuring that key events are captured.
2. Implement video summarization techniques that condense surveillance footage into clips highlighting notable actions or events, such as intruder detection, object movements, or specific zone breaches. This feature reduces the time needed for review by focusing on the most important moments.

## Secure remote monitoring for privacy-preserving surveillance video transmission

Problem: Most users likes to have remote monitoring access to the space, property or whatever it is they are interested in monitoring but they worry about hacks and video leaks which poses privacy concerns. For this reason they then to avoid third-party cloud services and turning to local video surveillance as a more secure option. The challenge here is to develop a system that allows secure, encrypted remote access to surveillance footage while minimizing privacy risks, ensuring that sensitive video data is transmitted securely.

Proposed Solution: A locally hosted surveillance system that ensures data privacy by keeping footage and metadata on-site while still allowing remote access via secure, encrypted channels. This balances the need for privacy with the convenience of remote monitoring.

Related Work

Solution

# **Target Users**

1. Homeowners and residential users
2. Organizations/ institution

**Scenario based Use Case for institution**:

hotels, banks

Institutions with valuable inventory can leverage motion-triggered recording to monitor all access to money vault, storage rooms. Immediate alerts can be sent to local security guard for video review and if an anomaly is captured, they can swing into action to de-escalate the situation in time

**Benefit**:

**This system reduces the footprint of security guards.**

**Security Focus are always shifted to where it is wanted the most, therefore improving efficiency.**

**The response time of security agents are improved and so threat can be handled quick and losses minimized.**

**Labs, storage areas of factories**

If an individual stays too long in position marked as critical area such as storage space containing dangerous and hazardous materials then this could be a sign that the individual be in danger and needs immediate intervention

**Benefit**:

**Surveillance system use alert functionality to provide timely intervention to arrest a life threaten situation.**

**This video encryption solution used in surveillance system ensure that the videos of people in such kind of situation is secured and cannot leak out to the public to cause privacy issues for individual and company.**

# References List

[1] S. Abdurrahman, “Smart video-based surveillance: Opportunities and challenges from image processing perspectives,” pp. 10–10, 2017, doi: 10.1109/icitacee.2016.7892400.

[2] H. Sharma and N. Kanwal, “A Survey of Object Detection Techniques for Improving Smart Surveillance,” *Proc. IEEE Int. Conf. Image Inf. Process.*, pp. 603–609, 2023, doi: 10.1109/ICIIP61524.2023.10537696.

[3] S. Agrawal and P. Natu, *ABGS Segmenter: pixel wise adaptive background subtraction and intensity ratio based shadow removal approach for moving object detection*, vol. 79, no. 7. 2023. doi: 10.1007/s11227-022-04972-9.

Things to search for during literature review

1. Target user and domain
2. Problem solved by project
3. Further work
4. Technologies used
5. Privacy consideration

# Target Users

## **Homeowners and Residential Users**

Use case:

Homeowners aiming to enhance the security of their properties can significantly benefit from a locally hosted surveillance system equipped with remote monitoring capabilities, ensuring their privacy is not compromised.

This system is designed to send immediate alerts when potential intruders are detected or when non-intruders remain in critical areas for extended periods, indicating suspicious activity. This proactive approach not only enhances security but also empowers homeowners to respond quickly to potential threats.

Furthermore, the surveillance system facilitates efficient video management by automatically saving only motion-triggered clips. This functionality enables users to effectively review and archive footage, significantly reducing the time spent searching for relevant incidents and the storage space required for video data. By prioritizing essential recordings, homeowners can access crucial evidence without the hassle of sifting through hours of inactive footage.

## **Organizations and Institutions**

**Use Case Scenario**:

**Hotels and Banks**: Institutions with valuable assets can leverage motion-triggered recording to monitor critical access points, such as money vaults and storage rooms. Immediate alerts can be sent to local security personnel for video review. If an anomaly is detected, security agents can swiftly intervene to de-escalate potential threats.

**Benefits**:

* Reduces the operational footprint of security personnel.
* Allows security focus to shift to areas where it is most needed, enhancing overall efficiency.
* Improves the response time of security agents, enabling quick threat management and minimizing potential losses.

**Laboratories and Storage Areas in Factories**: In environments where hazardous materials are stored, the system can monitor individuals who linger in critical areas. If someone remains too long in a designated danger zone, alerts can prompt immediate intervention.

**Benefits**:

* The surveillance system’s alert functionality enables timely action, potentially preventing life-threatening situations.
* The video encryption features ensure that footage remains secure, protecting the privacy of individuals and the integrity of the organization.
  + **1**. A homeowner who is away can always have an eye on what’s happening in their home. They can rely on this system to receiving alerts and video clips only when motion is detected without worries over preserving privacy by avoiding cloud-based services.
  + **2**. Users who do not want to spend so much in
  + **Benefit**: These users often seek reliable and affordable surveillance systems to monitor their property and valuables. This project provides enhanced security features such as real-time alerts, intelligent motion detection, and local storage options that maintain privacy while offering the advantage of remote monitoring. It addresses privacy concerns by keeping data in-house and ensures that even low-budget homeowners can benefit from advanced security without relying on expensive third-party services or cloud storage.

**Human vs. Animal Classification**: Look into projects that focus on object detection and classification using computer vision. The goal here is to identify what kind of intruder is entering a room and their characteristics. There may be implementations using YOLO, TensorFlow, or **OpenCV-based classifiers**.

#### 4. **Human and Animal Detection**

* Focus on the application of **deep learning models** (e.g., TensorFlow or PyTorch) for intruder classification.
* Research pre-trained models like **YOLO (You Only Look Once)** for real-time object detection or **HOG (Histogram of Oriented Gradients)** with SVM for human detection.
*  In a human detection model, MobileNet can be paired with SSD (Single Shot MultiBox Detector) as the detection head, creating a streamlined pipeline suitable for real-time processing on a CPU.
*  Alternatively, MobileNet can be combined with YOLO (You Only Look Once) for tasks requiring higher frame rates, though MobileNet-SSD remains a more lightweight option.

**Motion Detection and Tracking**: Study the use of advanced algorithms such as **Kalman Filters** or **Optical Flow** for precise motion tracking.

**daptability**: Implement **adaptive thresholding** and **histogram equalization** to adjust the sensitivity of the motion detection algorithm in different lighting conditions. Techniques like **Gamma correction** can further enhance visibility in low light or overly bright environments.

Phase 1: Initialize the reference frame for the background subtraction model

This phase is useful to generate a background frame called a reference frame from

the initial few frames in consideration of not having moving objects in those frames.

In this research work, we adapt the concept of the pixel-based averaging method

to generate the background frame by automatically calculating the initial threshold

value. Here, we consider B(x) initial frames { *B*1(x), *B*2(x), ….*Bn*−1(x), *Bn*(x)} where

x represents the location of pixels in the frame. We calculate the Mean \_*M*1(*x*)\_ by

using Eq. (1) and Variance \_*V*1(*x*)\_ by using Eq. (2) of first frame to understand the

statistical behavior of each pixel in the frame.

eqn 1

eqn 2

An initial threshold is computed by using Eq. (3) to generate the reference frame.

This step is used for the pixels’ segmentation to generate the background frame.

eqn 2

The entire process of creating the initial background model for initial frames is

summarized in Algorithm 1.

Literature review

Similar project

Technique and methods :-

MOG2, frame differencing, YOLOv3 (object detection), Kalman filter (object tracking), openCV,

1. Research for lighting conditions improvement

**Studying showing the effectiveness of my approach**