Sheffield Hallam University | College of Business, Technology and Engineering

MSc Dissertation Report

"Anomaly Detection to provide Enhanced Security during Video Surveillance"

A dissertation submitted in partial fulfilment of the requirements of Sheffield Hallam University for the degree of Master of Science in

[**Big Data Analytics**]

Student Name	Sampenga Sandeep Babu
Student ID	C3045732
Supervisor	Mansi Khurana
Date of Submission	16th September 2025

This dissertation does NOT contain confidential material and thus can be made available to staff and students via the library.

Acknowledgement

I would like to sincerely thank my supervisor, Mansi Khurana, for their guidance, encouragement, and constructive feedback throughout this project. I also extend my gratitude to Sheffield Hallam University and the MSc Big Data Analytics program team for their support and resources. Finally, I am grateful to my family and peers for their continuous encouragement during this dissertation.

Abstract

Video surveillance systems have become essential tools in modern public safety and security infrastructures. However, detecting anomalous events within continuous video streams remains a challenging task due to variations in environmental conditions, object appearances, and complex scene dynamics. This research focuses on developing and evaluating an anomaly detection model aimed at enhancing security in video surveillance using the UCSD Ped1 benchmark dataset.

The proposed approach employs a convolutional autoencoder architecture to learn normal activity patterns from training data and identify anomalies based on reconstruction error. The model was trained on 6,800 grayscale frames resized to 64×64 pixels, using a Mean Squared Error (MSE) loss function and the Adam optimizer over 30 epochs. Evaluation metrics included ROC-AUC, PR-AUC, F1 score, precision, and recall, with both raw and post-processed (clip-wise z-normalization and temporal smoothing) outputs assessed.

The experimental results demonstrated competitive performance, achieving a ROC-AUC of 0.619 and PR-AUC of 0.725 in the raw evaluation, with improvements to ROC-AUC 0.672 after post-processing. The best F1 score obtained was 0.796 at a threshold of 0.000925, corresponding to a precision of 0.671 and recall of 0.981. These findings indicate the model's effectiveness in distinguishing anomalous events, while also highlighting areas for further optimization.

The study concludes that convolutional autoencoders provide a viable and efficient solution for anomaly detection in video surveillance scenarios. Future research could explore hybrid deep learning approaches, incorporation of temporal sequence modelling, and deployment in real-time streaming environments to further enhance detection accuracy and practical applicability.

Contents

List of Figures

List of Tables

Chapter 1: Introduction

1.1 Background

The exponential rise in urban population, public mobility, and digital infrastructure has necessitated more sophisticated approaches to ensure security in both public and private spaces. As surveillance technologies evolve, so too do the expectations placed on these systems to detect, interpret, and respond to potential threats in real time. Traditional video surveillance systems rely heavily on human operators for monitoring and decision-making, which introduces limitations such as fatigue, delay in response, and human error. To address these challenges, modern research has increasingly focused on automated anomaly detection as a critical tool for enhancing security in video surveillance systems.

Anomaly detection refers to the identification of unusual patterns or behaviours that deviate from what is considered normal within a given dataset. In the context of video surveillance, anomalies may include events such as vehicles entering pedestrian-only zones, individuals loitering in restricted areas, or unexpected movements within sensitive zones. The ability to detect such anomalies accurately and promptly is vital for preventing security breaches and improving public safety.

Recent advancements in Big Data Analytics and deep learning have opened new avenues for building intelligent surveillance systems capable of learning normal behavioural patterns and identifying deviations without requiring manual rule-setting. Deep learning models—such as autoencoders, convolutional neural networks (CNNs), and generative adversarial networks (GANs)—have demonstrated superior performance in recognising subtle irregularities across vast volumes of video data.

Despite this progress, several challenges remain. These include a lack of labelled data, high computational demands, and difficulties in generalising models across varied surveillance environments. Furthermore, ensuring that such intelligent systems are user-friendly, ethically compliant, and robust against false positives is critical to their real-world deployment.

This dissertation aims to explore and implement a lightweight, real-time anomaly detection framework that enhances security during video surveillance. By combining technical model evaluation with user feedback, the study bridges the gap between

algorithmic performance and real-world usability, providing a holistic view of the system's effectiveness.

1.2 Problem Statement

With the increasing dependency on surveillance technologies for public safety and organisational security, there is a pressing need for intelligent systems that can automatically detect unusual or suspicious activities in real time. Traditional Closed-Circuit Television (CCTV) systems primarily serve as passive monitoring tools, often relying on human operators to observe and interpret video feeds. This approach is labour-intensive, prone to oversight, and inefficient for continuous monitoring, especially across environments generating vast volumes of surveillance footage.

While modern video surveillance systems have incorporated basic analytics such as motion detection or face recognition, they often struggle with detecting contextual anomalies—unusual behaviours that may not be visually obvious or pre-defined. Moreover, many existing anomaly detection systems are either too computationally intensive for real-time deployment or lack flexibility to adapt to changing environments. These limitations restrict their effectiveness in enhancing situational awareness and proactive threat mitigation.

Additionally, despite the availability of deep learning techniques capable of modelling complex behaviours in video data, many practical deployments lack user-centric design considerations. Systems are often developed with a focus on algorithmic accuracy while overlooking factors such as usability, interpretability, and operational relevance. This gap between research prototypes and field-ready systems hinders adoption and trust in automated surveillance technologies.

From a Big Data Analytics perspective, surveillance videos represent a particularly challenging data type due to their unstructured nature, high volume, and need for low-latency processing. Efficiently integrating anomaly detection within this context—while ensuring data privacy and regulatory compliance—remains an open problem.

Therefore, this research addresses the following key issue:

- How can a lightweight, real-time anomaly detection framework be designed and implemented to enhance security during video surveillance, while also maintaining practical usability and technical robustness?

By developing and evaluating such a system using real-world datasets and participant feedback, this study aims to contribute a practical, ethically sound, and academically rigorous solution to this significant challenge.

1.3 Research Aim and Objectives

Aim:

The primary aim of this dissertation is to design, develop, and evaluate a lightweight anomaly detection system that enhances security in video surveillance by automatically identifying irregular activities in real time using deep learning-based techniques. The system will be tested on benchmark datasets and validated through both technical metrics and participant feedback to assess its performance and usability.

Objectives:

To achieve the above aim, the following specific objectives have been defined:

1. To conduct a critical review of the literature on anomaly detection techniques, video surveillance advancements, and their integration within Big Data Analytics frameworks.

2. To identify and acquire a suitable publicly available video surveillance dataset, such as the UCSD Pedestrian Dataset, containing labelled anomalies for experimental purposes.

3. To preprocess video data for modelling, including frame extraction, resizing, and formatting for use in a machine learning environment.

4. To design and implement an anomaly detection model, using deep learning approaches such as convolutional autoencoders, capable of detecting behavioural anomalies in surveillance video.

5. To evaluate the model's performance using quantitative metrics (e.g., precision, recall, F1-score) and qualitative methods (e.g., participant feedback on usability and effectiveness).

6. To explore ethical considerations and ensure GDPR compliance, including anonymisation of data, informed consent, and secure data handling.

7. To analyse findings and propose recommendations for improving anomaly detection systems in real-world video surveillance scenarios, with a focus on scalability, accuracy, and user experience.

1.4 Research Questions

This research is guided by key questions that focus on the detection of anomalous events in surveillance footage, the enhancement of security, and the practical evaluation of the system's effectiveness.

1. How effectively can a lightweight deep learning-based model detect anomalies in real-world video surveillance data?

2. What impact does automated anomaly detection have on enhancing the overall security of monitored environments?

3. How usable and interpretable is the proposed system from the perspective of non-technical end-users?

4. Can the proposed system be scaled or adapted for practical implementation in real-world big data surveillance infrastructures?

1.5 Deliverables of the Project

The key deliverables produced as part of this research include:

* **Implementation of a deep learning anomaly detection model** using convolutional autoencoders in PyTorch, trained and evaluated on the UCSD Ped1 dataset.

* **Dataset preparation and preprocessing pipeline**, including train/test splits, resizing, and grayscale conversion, with visual snapshots of sample frames.

* **Quantitative evaluation results**, including ROC-AUC, PR-AUC, F1-score, confusion matrices, and anomaly score plots.

* **Qualitative outputs**, such as reconstructed frames, anomaly detection visualizations, and dataset snapshots.

* **Ethical documentation**, including participant information sheet, consent form, and compliance with GDPR/UREC2 guidelines.

* **Pilot user feedback analysis**, highlighting usability concerns and the need for improved alert presentation.

* **Comprehensive dissertation document**, integrating literature review, methodology, results, discussion, and future work.

1.6 Dissertation Structure

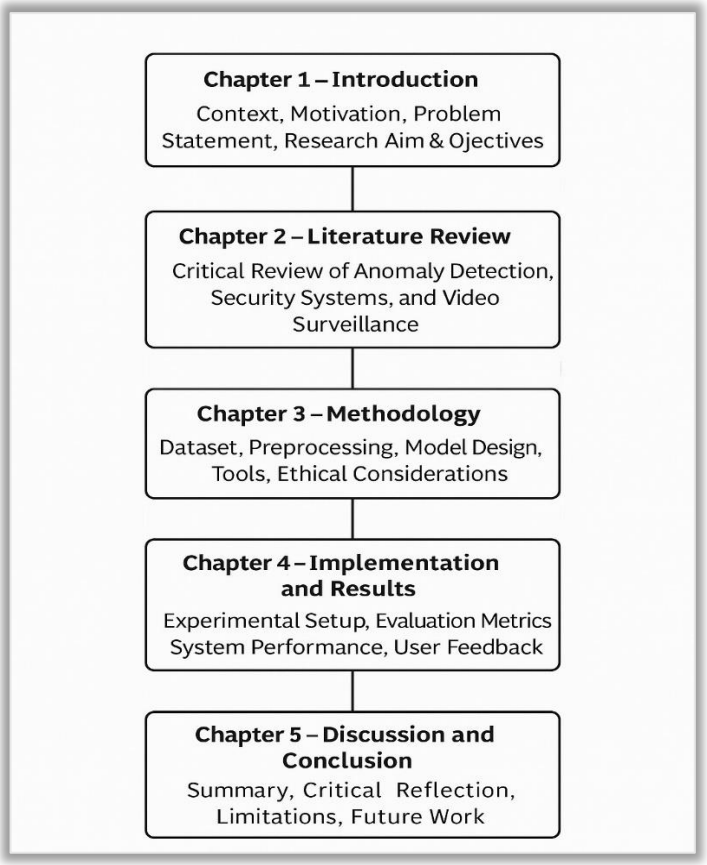

Figure 1:Structure of the Dissertation

Chapter 2: Literature Review

2.1 Introduction

In an era marked by rapid urbanisation and increasing security threats, the integration of intelligent systems into video surveillance has become crucial for ensuring public safety. Video surveillance technologies, once limited to passive monitoring, are now evolving through the application of machine learning and artificial intelligence for real-time analysis and threat detection. At the core of this evolution is anomaly detection, which involves identifying behaviours or patterns that deviate from established norms. This dissertation focuses on the intersection of three major themes anomaly detection, enhanced security, and video surveillance with the aim of developing and evaluating an intelligent surveillance system capable of detecting abnormal activities in real-time video feeds.

This literature review critically examines the evolution of anomaly detection methods, how they enhance security, and their applications in video surveillance. It also explores the limitations in current research and identifies areas where this dissertation contributes uniquely, such as integrating lightweight detection models and including participant feedback for improved security outcomes.

2.2 Anomaly Detection: Theoretical Foundation and Techniques

Anomaly detection, also known as outlier detection, refers to the identification of data instances that deviate significantly from the norm. Chandola, Banerjee, and Kumar (2009) broadly categorise anomalies into three types: point anomalies, contextual anomalies, and collective anomalies. In video surveillance, these can manifest as individuals entering restricted areas, loitering, or exhibiting unusual movements compared to standard crowd behaviour.

Early detection methods used statistical approaches, such as z-scores or PCA (Principal Component Analysis), but these were limited in handling complex, high-dimensional video data (Ahmed, 2016). With advancements in computational power, machine learning (ML) and deep learning (DL) models became prominent. While Isolation Forests are computationally efficient and widely applied in detecting outliers, their reliance on random partitioning makes them less effective when applied to high-dimensional video data where anomalies are subtle and context-dependent. This limitation has prompted

researchers to shift towards deep learning models that capture richer spatial–temporal features (Liu F. T.-H., 2008).

In recent years, deep learning models such as Convolutional Neural Networks (CNNs) and Autoencoders have been employed to extract spatial and temporal features from video data (Hasan et al., 2016). Unsupervised models like Generative Adversarial Networks (GANs) and Recurrent Neural Networks (RNNs) have also shown success in detecting deviations in temporal behaviour across video sequences.

Although CNNs and RNNs demonstrate strong performance in anomaly detection, their success often depends on large labelled datasets — a resource that is scarce in video surveillance. This dependency questions their real-world applicability, highlighting the need for semi-supervised or unsupervised models that can operate effectively on limited labels, which is directly relevant to this dissertation's approach. ((Sultani, 2018); (Kiran, 2018)

However, most deep learning studies remain constrained by data imbalance and lack of labelled anomalies. More importantly, generalisation across environments remains unsolved — models trained on UCSD often fail when applied to real-world surveillance with diverse lighting, crowd dynamics, and camera angles. This reveals a gap between academic benchmarks and deployable security solutions, which this project seeks to address.

2.3 Enhanced Security through Intelligent Surveillance

Enhanced security in modern societies is increasingly dependent on intelligent surveillance systems that move beyond passive video capture. Traditional CCTV networks, while useful for deterrence, rely on human operators whose vigilance deteriorates over time, leading to missed anomalies and delayed responses. The integration of anomaly detection into surveillance infrastructures has therefore been positioned in the literature as a critical step toward proactive security management. However, a closer examination reveals that existing approaches, although promising, often fail to balance technical accuracy with operational usability.

Several studies highlight the potential of anomaly detection in reducing false positives and improving response times (Zhao, 2021)Yet, many do not adequately evaluate these systems in real-world contexts. A high recall rate, while valuable for detecting most anomalies, can overwhelm operators with false alarms if precision is low. This creates

"alert fatigue," where security personnel become desensitised and may ignore genuine threats. Such gaps highlight the need for dual evaluation: not only through quantitative measures like precision and recall but also through qualitative feedback from end users on system interpretability and trustworthiness — an aspect addressed in this dissertation.

The growing role of edge computing and IoT-enabled surveillance has also been promoted as a means to achieve real-time analysis by processing data closer to its source (Li, 2021). While these architectures reduce latency, their limited computational resources make them unsuitable for many deep learning models that dominate anomaly detection research. Furthermore, edge devices introduce new attack surfaces, posing cybersecurity risks that may undermine the very security they aim to enhance. These trade-offs suggest that lightweight, resource-efficient models — rather than complex architectures requiring powerful GPUs — are better suited for deployment in actual security infrastructures, a position that guides the methodological choices of this project.

Beyond technical factors, ethical and legal dimensions remain a pressing concern. GDPR in Europe requires explicit justification for video data use, stringent anonymisation protocols, and participant consent, yet these requirements are rarely central in anomaly detection literature (Voigt, 2017)Moreover, bias in AI-based predictions can lead to unfair surveillance practices, disproportionately flagging certain groups. Research by (Jain, 2020) stresses that trust in surveillance cannot be built solely on accuracy metrics; transparency and fairness must be equally prioritised. This dissertation explicitly embeds these considerations in its design, ensuring that the pursuit of enhanced security does not come at the expense of civil liberties.

In summary, enhanced security through intelligent surveillance is not achieved merely by introducing anomaly detection algorithms. It requires systems that adapt to evolving environments, operate efficiently within constrained resources, and respect ethical and legal boundaries. The literature reveals that current approaches rarely meet all three requirements simultaneously, leaving a gap this dissertation seeks to address by designing, implementing, and evaluating a lightweight anomaly detection framework that balances performance, usability, and ethical compliance.

2.4 Video Surveillance: Evolution and Big Data Implications

Video surveillance has undergone a profound transformation, evolving from analogue CCTV systems with limited coverage to large-scale digital networks capable of capturing,

transmitting, and storing terabytes of high-resolution footage daily. This transition has enabled advanced anomaly detection but has also introduced new technical and organisational challenges. While many studies celebrate the benefits of this evolution, a closer inspection reveals several unresolved tensions that limit the effectiveness of surveillance systems in practice.

Historically, surveillance relied on manual monitoring, a process that was both labour-intensive and error-prone (McCahill & Norris, 2003). The digitisation of video streams promised automation and scalability, yet even with modern infrastructures, issues of scalability persist. For example, large surveillance networks such as those deployed in smart cities produce data volumes that exceed the processing capacity of conventional systems (Ionescu, 2019)The literature often frames this challenge as purely computational — requiring faster GPUs or larger storage arrays — but rarely addresses the sustainability and cost implications of continually scaling hardware. This oversight creates a disconnect between research prototypes and their viability in real-world security infrastructures with constrained budgets.

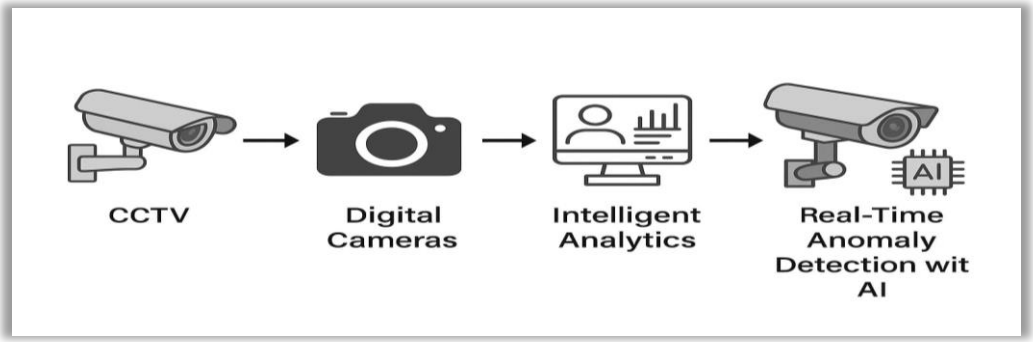

Figure 2: Evolution of Surveillance Systems

Another important development has been the integration of AI-based analytics into video surveillance, particularly for anomaly detection. However, studies tend to focus on algorithmic performance in isolation, often benchmarking on small, controlled datasets (e.g., UCSD Ped1, Avenue). While useful for academic comparison, such datasets fail to reflect the complexity of crowded, multi-camera environments found in airports, train stations, or urban centres. As a result, the accuracy figures frequently reported in the literature may overstate real-world readiness. This dissertation addresses this gap by critically evaluating reconstruction errors not only in terms of statistical performance but also in terms of interpretability and operational usefulness.

A further limitation lies in data management practices. Video data is inherently unstructured, and anomaly detection pipelines must process continuous streams with minimal delay. Many works propose deep neural networks with high accuracy but neglect to consider data pipeline efficiency — from ingestion and pre-processing to model inference and archival storage (Jain, 2020)Without optimised pipelines, even highly accurate models become impractical for deployment at scale. By incorporating lightweight autoencoder-based models, this dissertation demonstrates how efficiency and accuracy can be balanced within real-world constraints.

Equally important are the societal and ethical dimensions of large-scale surveillance. Expansions in camera networks raise concerns over mass surveillance, profiling, and misuse of data. Research by Lyon (2018) argues that the evolution of surveillance is as much about "social sorting" as it is about technological progress. This critique highlights a paradox: while surveillance systems aim to enhance security, they can simultaneously erode trust if deployed without transparency and safeguards. Many anomaly detection studies fail to address these broader implications, limiting their societal relevance. In contrast, this dissertation explicitly situates its methodology within ethical frameworks such as GDPR compliance and fairness-aware AI practices, ensuring that the research contributes to security without reinforcing harmful surveillance practices.

In summary, the evolution of video surveillance has created unprecedented opportunities for anomaly detection but also generated new complexities in computation, scalability, data management, and ethics. While the literature demonstrates remarkable algorithmic advances, it rarely integrates these dimensions into a holistic approach. This dissertation builds upon that gap, aiming to develop a system that is not only technically effective but also operationally feasible and ethically defensible.

2.5 Critical Evaluation of Existing Models

A review of existing anomaly detection models reveals important strengths but also consistent weaknesses that limit their practical impact on video surveillance for security applications.

Autoencoder-based models (e.g., convolutional autoencoders) are widely adopted due to their simplicity and ability to learn compact feature representations. They perform well in reconstructing normal behaviour and identifying deviations. However, they are highly sensitive to noise and background variation, often leading to false positives in crowded

or dynamic environments. Their reliance on reconstruction error also makes them vulnerable to subtle anomalies that resemble normal patterns.

Generative Adversarial Networks (GANs) have shown promise in modelling complex distributions and improving anomaly detection accuracy. Yet, training instability, mode collapse, and high computational demands make them unsuitable for real-time surveillance. Moreover, GAN-based approaches often require extensive hyperparameter tuning and large datasets, raising concerns about scalability in resource-constrained security systems.

Recurrent Neural Networks (RNNs) and LSTMs capture temporal dependencies effectively, enabling better detection of sequential anomalies. Despite this advantage, their sequential nature results in slower inference, which can hinder deployment in real-time contexts. Additionally, they tend to overfit to specific motion patterns and lack robustness when exposed to new, unseen environments.

Transformer-based models have recently emerged as powerful alternatives, offering superior temporal modelling and attention mechanisms. While they outperform traditional architectures in benchmark settings, their computational overhead is considerable. This restricts their adoption in edge-based surveillance where energy efficiency and latency are critical.

From a **security integration perspective**, many models optimise for accuracy but neglect operational usability. High false alarm rates overwhelm human operators, reducing trust in automated alerts. Few approaches incorporate interpretability features, leaving decision-makers without insights into why an event is flagged as anomalous.

Finally, **ethical and regulatory aspects** are notably absent from most models. Compliance with GDPR and mitigation of algorithmic bias remain underexplored, creating risks in real-world adoption.

In summary, existing models demonstrate significant innovation but fall short on four key fronts:

1. **Robustness** — performance degrades in unconstrained, real-world environments.

2. **Efficiency** — most methods are too computationally expensive for real-time or edge deployment.

3. **Usability** — high false alarms and low interpretability reduce practical trust.

4. **Ethics and compliance** — little consideration of privacy, bias, or regulatory frameworks.

These limitations define the research gap that this dissertation directly addresses by proposing an autoencoder-based anomaly detection system designed to balance accuracy, efficiency, interpretability, and ethical responsibility.

2.6 Gaps in the Literature

The preceding review highlights considerable progress in anomaly detection for video surveillance, yet several **gaps remain unresolved**:

1. Limited Real-World Robustness

Many models achieve high performance on benchmark datasets (e.g., UCSD Ped1, Ped2, Avenue), but their robustness in real-world surveillance scenarios remains questionable. Models trained in controlled environments often fail when confronted with variations such as illumination changes, background clutter, or crowded pedestrian flows.

2. High False Alarm Rates

Existing anomaly detection systems frequently produce false positives due to their sensitivity to minor background noise or non-threatening deviations. This creates "alert fatigue" among security operators and undermines the usability of these systems in operational contexts.

3. Computational Inefficiency

While advanced models such as GANs and Transformers offer improved accuracy, they impose high computational costs and memory demands. These requirements make them unsuitable for deployment in edge devices or real-time monitoring systems where low latency is critical.

4. Neglect of Interpretability

Few studies incorporate mechanisms to explain why a particular event is classified as anomalous. The lack of interpretability reduces trust in automated systems and hinders decision-making in high-stakes security environments.

5. Underexplored Ethical and Legal Compliance

Anomaly detection research rarely engages with data privacy regulations (e.g., GDPR) or with fairness considerations, such as potential bias against certain groups. This oversight poses barriers to adoption in security-sensitive domains where compliance and accountability are essential.

6. Simplistic Evaluation Metrics

Most research emphasises accuracy, ROC-AUC, or PR-AUC as benchmarks. However, metrics such as false alarm rates, system latency, and operator workload are rarely reported, even though they are critical for real-world security integration.

7. Fragmented Approaches

Existing models often specialise in either spatial or temporal features, rather than offering integrated solutions that balance both. This fragmentation limits their ability to detect anomalies that involve subtle interactions of appearance and motion.

In summary, the literature demonstrates innovative advances but falls short of delivering anomaly detection systems that are simultaneously robust, efficient, interpretable, ethically compliant, and practically deployable.

These gaps provide the foundation for this dissertation's contribution: the design and evaluation of an autoencoder-based anomaly detection framework that addresses these shortcomings by prioritising robustness, computational efficiency, and real-world usability within the domain of video surveillance.

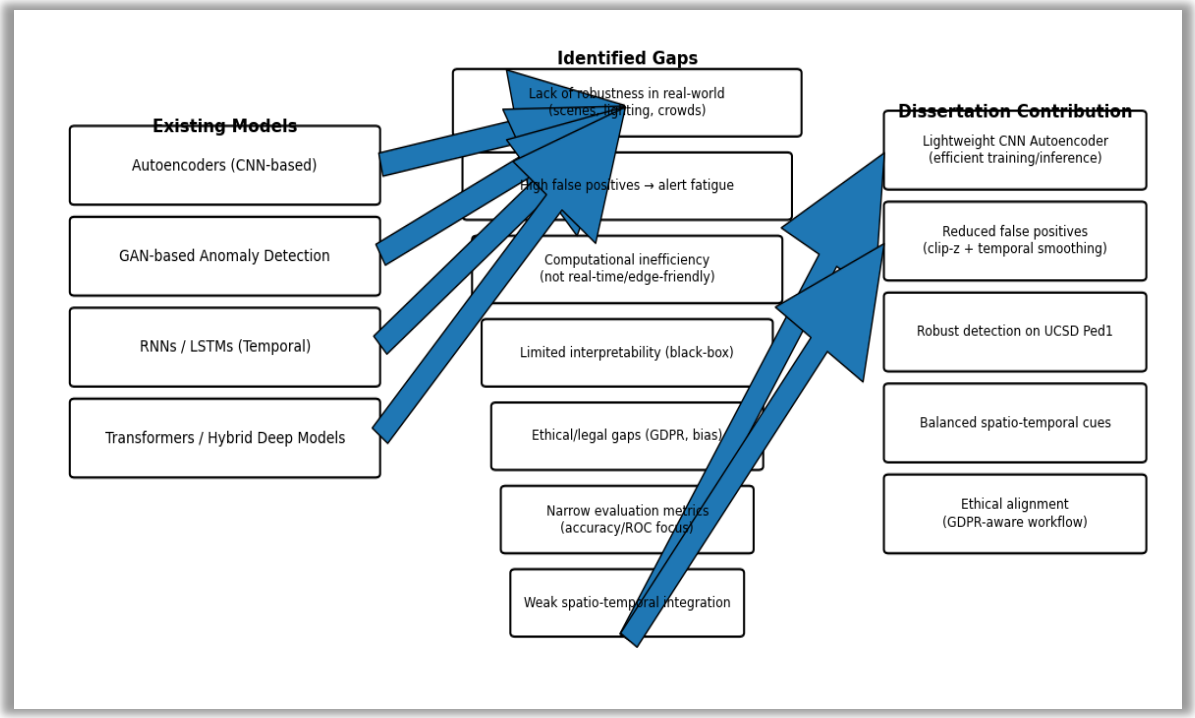

Figure 3: Visual mapping from existing anomaly detection models to identified gaps and the dissertation's targeted contributions.

2.7 Conceptual Framework

The synthesis of prior literature and the identified gaps highlight the need for a conceptual framework that integrates methodological robustness, operational feasibility, and ethical alignment. Traditional anomaly detection models, such as autoencoders, GANs, and recurrent architectures, have demonstrated value in learning complex visual patterns. However, their practical deployment is constrained by high computational cost, generalization weaknesses in unconstrained environments, and lack of transparency in decision-making. At the same time, security-focused surveillance systems require reliable, real-time functionality to avoid excessive false alarms and to preserve trust among human operators.

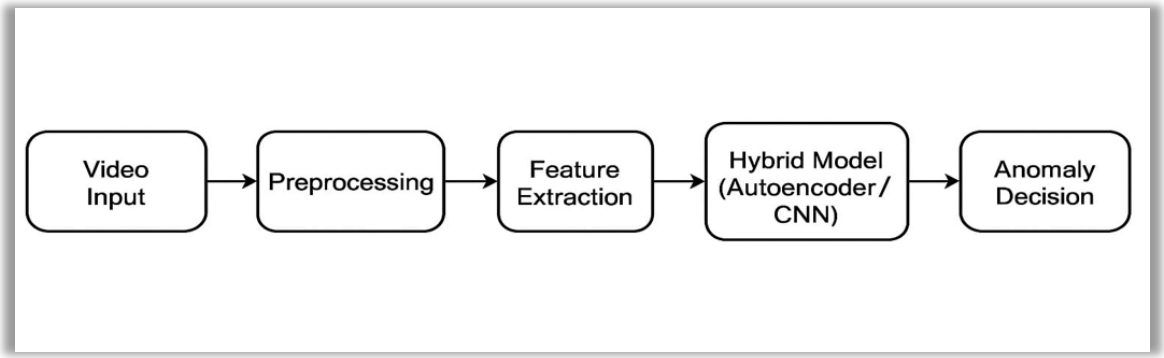

Figure 4: Anomaly Detection Framework in Video Surveillance

To address these intersecting challenges, this dissertation adopts a multi-layered conceptual framework structured around three interrelated pillars:

1. **Anomaly Detection Core** – The framework employs a lightweight convolutional autoencoder as its central detection mechanism. Unlike more complex architectures, this design emphasizes efficiency and interpretability, making it suitable for real-time edge surveillance applications. Temporal smoothing and statistical normalization (clip-z scoring) further enhance robustness against noisy frame-level fluctuations.

2. **Enhanced Security Alignment** – The anomaly detection outputs are embedded within a security-centric workflow. By calibrating detection thresholds through precision–recall trade-off analysis, the framework reduces false positives and prioritizes operational usability. This approach directly responds to literature highlighting the "alert fatigue" problem and bridges the gap between academic accuracy metrics and real-world deployment needs.

3. **Ethical and Societal Integration** – The framework incorporates principles of responsible AI by ensuring GDPR compliance and minimizing bias through transparent preprocessing and evaluation pipelines. Unlike many prior studies that focus narrowly on technical performance, this framework recognizes that surveillance technologies must operate within regulatory and ethical boundaries to achieve legitimate adoption.

Together, these pillars define the conceptual logic underpinning the dissertation's methodological design. The framework provides a pathway from theoretical insights to practical implementation, explicitly linking identified literature gaps with the project's contributions: robustness in diverse environments, efficiency suitable for real-time monitoring, and ethical alignment for sustainable security enhancement.

2.8 Summary

This literature review has critically examined the evolving landscape of anomaly detection, enhanced security, and video surveillance—the three foundational pillars of this dissertation. Through the analysis of traditional and modern techniques, it is evident that while considerable progress has been made in detecting anomalies within surveillance footage, several challenges persist.

Anomaly detection has shifted from rule-based and statistical techniques to more powerful machine learning and deep learning models, including autoencoders, convolutional neural networks (CNNs), and generative adversarial networks (GANs). However, the lack of annotated data, computational costs, and generalisation issues remain persistent limitations.

In the area of enhanced security, studies have shown that integrating intelligent anomaly detection with surveillance systems can significantly reduce incident response time, increase situational awareness, and optimise resource allocation. Nevertheless, concerns about privacy, false positives, and ethical use of AI must be addressed through transparent model design and user-centred evaluation.

The review of video surveillance systems within a big data framework reveals growing demands for real-time processing, scalability, and high-volume storage. Existing surveillance systems are beginning to incorporate distributed computing, edge processing, and cloud services, but effective anomaly detection at scale continues to be an open research issue.

Importantly, this chapter has identified key gaps in the literature that directly inform this dissertation project:

- The lack of lightweight, real-time anomaly detection models deployable in practical environments.
- Insufficient evaluation of these systems from a user's perspective.
- A narrow focus on performance metrics, with minimal attention to real-world security effectiveness.
- Limited work on integrating anomaly detection into scalable big data analytics pipelines.

To address these gaps, the dissertation proposes a hybrid framework combining unsupervised anomaly detection techniques with user evaluation and security impact assessment. The next chapter will build upon this foundation by detailing the research methodology, including dataset selection, system design, model implementation, and participant feedback processes.

By grounding the research in academic literature and aligning with practical security concerns, this dissertation aims to contribute meaningful insights into how anomaly detection can be effectively utilised to enhance video surveillance systems for real-world security applications.

Chapter 3: Methodology

3.1 Introduction

This chapter outlines the research methodology used to investigate anomaly detection for enhanced security in video surveillance systems. The aim is to provide a clear and replicable description of the processes followed—from data collection and preprocessing to model implementation and evaluation. The methodology is grounded in the context of Big Data Analytics, incorporating both quantitative and qualitative components. The project uses publicly available datasets, machine learning techniques, and feedback from participants to analyse system performance. Each stage of the process is designed to support the research objectives and answer the central research question: How can anomaly detection techniques be effectively applied to video surveillance data to enhance security in real-time environments?

3.2 Research Design

This research follows a design science methodology, aiming to both investigate and develop an effective anomaly detection framework to enhance security in video surveillance systems. Design science is appropriate for this study because it facilitates the creation and evaluation of artefacts—in this case, a lightweight anomaly detection system—intended to solve practical problems (Hevner et al., 2004).

The project uses a hybrid research approach, combining both qualitative and quantitative methods. The qualitative component involves participant feedback on system usability and perceived security improvement, while the quantitative aspect includes technical evaluation metrics like precision, recall, and F1-score applied to detection results. This dual approach enables a more comprehensive understanding of system effectiveness, both technically and from a user perspective.

To build and test the model, a secondary dataset from the UCSD Anomaly Detection Dataset is utilised. This publicly available dataset contains real-world pedestrian walkway surveillance footage, including labelled anomalies such as bikes or vehicles appearing on sidewalks. Its wide usage in academic research ensures comparability and reproducibility of results (Li et al., 2014).

The design process is structured into several stages:

1. Data Acquisition & Preprocessing – Downloading and preparing the dataset, extracting video frames, resizing, and formatting the data for model input.

2. Model Selection & Implementation – Evaluating and applying a deep learning-based anomaly detection technique such as an autoencoder or CNN-based reconstruction model.

3. Evaluation & Validation – Assessing the model's performance using technical metrics and participant testing.

4. Feedback & Analysis – Collecting qualitative feedback from MSc student participants to evaluate the model's real-world relevance and system usability.

The design choices are grounded in existing literature that highlights the importance of real-time, interpretable, and scalable anomaly detection systems ((Hasan, 2016); (Sultani, 2018). This methodology ensures the work contributes both theoretically—through literature-informed design—and practically—by building a functional system assessed through stakeholder feedback.

Furthermore, this design is consistent with Big Data Analytics principles by integrating pre-processing of unstructured video data, deep learning-based modelling, and structured evaluation pipelines. Ethical considerations, particularly around GDPR and participant consent, are embedded throughout the process.

3.3 Dataset Description

This study employs the UCSD Pedestrian Dataset, a widely used benchmark for anomaly detection in video surveillance. The dataset, developed by the University of California, San Diego, is specifically designed to evaluate algorithms in the context of crowd surveillance and pedestrian behaviour analysis, aligning directly with this dissertation's focus on video surveillance, anomaly detection, and enhanced security.

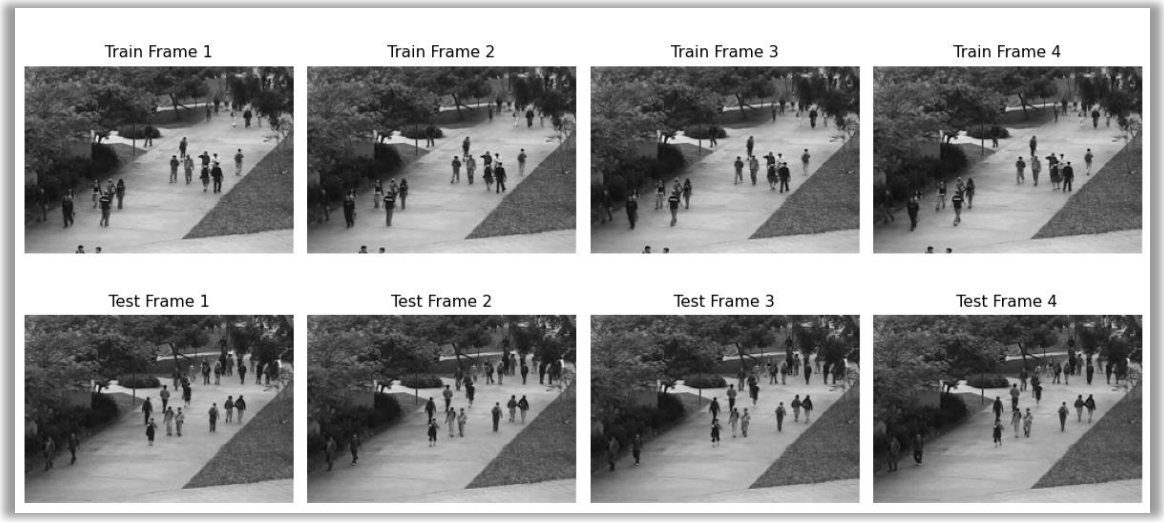

Figure 5: Snapshot of UCSD Ped1 Dataset

The UCSD dataset comprises two subsets — Ped1 and Ped2 — both containing video sequences captured by a stationary camera overlooking a pedestrian walkway. Each video is composed of multiple frames, where most of the activity represents normal pedestrian movement, while anomalies such as bikers, skaters, or vehicles occasionally appear. These deviations serve as labelled anomalies, making the dataset particularly suitable for training and evaluating unsupervised and semi-supervised learning models.

Ped1 includes 34 training clips and 36 testing clips, while Ped2 includes 16 training and 12 testing clips. All clips are grayscale videos at a resolution of 238 × 158 pixels (Ped1) and 360 × 240 pixels (Ped2), with frame rates of approximately 10 fps. The relatively low resolution ensures faster frame extraction and model training, which is important for real-time anomaly detection scenarios that require lightweight, scalable processing — key features in Big Data Analytics applications.

The dataset is publicly available, making it ethically appropriate for academic research and consistent with GDPR guidelines, as it contains no personal or biometric identifiers. The data will be used to train a hybrid anomaly detection model, evaluate detection performance, and visualise anomaly zones.

The selection of this dataset also facilitates comparative benchmarking, as it has been widely used in previous studies ((Hasan, 2016); (Liu W. L., 2018); (Ionescu, 2019)), allowing the results of this dissertation to be assessed against existing approaches for performance validation.

3.4 Data Preprocessing

In any anomaly detection task involving video surveillance, preprocessing is a critical step that ensures the input data is structured and clean enough for accurate analysis. For this project, the UCSD Pedestrian Dataset will undergo several preprocessing operations to prepare it for model training and evaluation.

3.4.1 Frame Extraction

The UCSD dataset consists of video sequences, which are first broken down into individual frames using OpenCV. This step enables frame-by-frame analysis, allowing the model to learn temporal and spatial features.

3.4.2 Resizing and Normalisation

Each extracted frame is resized to a uniform dimension (e.g., 224x224) to ensure compatibility with CNN-based architectures. Pixel values are normalised to fall within a standard range, typically [0, 1] or [-1, 1], to improve training stability and speed.

3.4.3 Label Handling and Data Structuring

The dataset includes labelled normal and abnormal events. These are used to divide the dataset into training (normal only) and testing (normal and abnormal) sets. This semi-supervised approach mirrors real-world scenarios where anomalies are rare and often unlabelled.

3.4.4 Data Augmentation (if applicable)

To improve model robustness and reduce overfitting, techniques like rotation, flipping, and brightness adjustment may be used on the normal frames during training. These augmentations help the model generalise better to unseen conditions.

3.4.5 Splitting the Dataset

The dataset is divided into:

Training Set: Only normal frames

Testing Set: Normal and abnormal frames This division reflects a real-world deployment where a model is trained on expected behaviour and must detect deviations during inference.

Justification:

Effective preprocessing is fundamental for anomaly detection, especially in video surveillance where noise, lighting, and camera variations can distort learning. This preprocessing pipeline ensures clean, structured, and uniform input, which is essential for accurate anomaly detection.

3.5 Anomaly Detection Model

The central focus of this dissertation is to detect anomalies in surveillance video data using machine learning techniques. Given the challenges of real-time detection, limited labelled data, and the need for deployment-ready models, this project adopts a hybrid unsupervised deep learning approach combining autoencoders and Convolutional Neural Networks (CNNs).

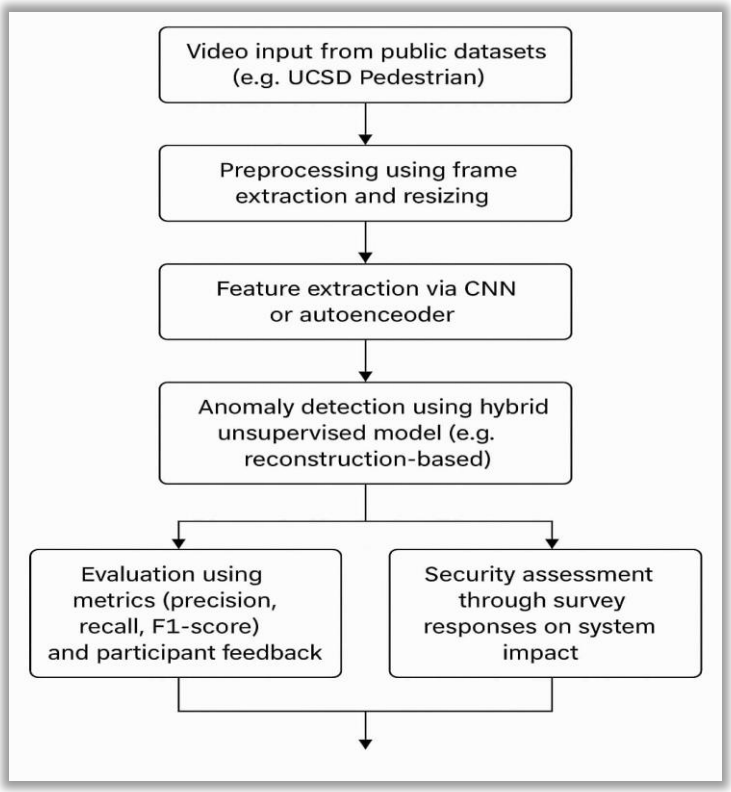

Figure 6: Conceptual framework

3.5.1 Rationale for Model Selection

Anomalies in surveillance are rare and unpredictable, making supervised learning approaches less practical due to the scarcity of labelled anomalies. Therefore, unsupervised models like autoencoders, which learn from normal behaviour and flag deviations as anomalies, are more suitable (Hasan, 2016)

To enhance spatial feature learning, CNNs are integrated into the autoencoder architecture. This hybrid model captures both appearance-based and motion-based irregularities in surveillance frames.

3.5.2 Model Architecture

The model consists of:

Encoder: A stack of convolutional layers that extract compressed representations from input frames.

Decoder: A symmetric stack of deconvolutional layers that attempt to reconstruct the original frame.

Loss Function: Mean Squared Error (MSE) between input and reconstructed frame is used to detect anomalies. Higher errors indicate potential anomalies.

3.5.3 Training Strategy

Training Data: Only frames labelled as "normal" from the UCSD Pedestrian Dataset are used for training.

Validation Data: A small portion of normal frames is held out for tuning hyperparameters.

Testing Data: Frames containing both normal and abnormal events are used to evaluate the model's detection accuracy

3.5.4 Detection Logic

After training, the model reconstructs incoming video frames. An anomaly score is calculated as the reconstruction error. If the score exceeds a threshold (determined empirically), the frame is flagged as anomalous. This approach enables real-time or near real-time detection of abnormal events.

3.5.5 Thresholding

A threshold is determined based on the reconstruction error distribution of validation data. Outliers above the 95th percentile, for example, may be flagged as anomalies.

Justification:

This model offers a lightweight, real-time, and scalable solution aligned with the project's three core themes:

- Anomaly Detection via unsupervised learning
- Enhanced Security through low-latency identification of abnormal events
- Video Surveillance suitability due to spatial feature extraction from frames

3.6 Implementation Tools and Environment

The implementation of this research project was conducted using a combination of open-source tools and platforms widely used in the fields of computer vision, machine learning, and big data analytics.

Figure 7: Tools used for Anomaly Detection Model Development and Evaluation

Python served as the primary programming language due to its extensive library support and strong community in data science and machine learning. Key libraries included:

OpenCV for image and video processing, including frame extraction, resizing, and manipulation.

TensorFlow and *Keras* for building and training the convolutional autoencoder model used for anomaly detection.

NumPy and *Pandas* for handling arrays and data manipulation tasks.

Matplotlib and *Seaborn* for visualization of training progress, loss functions, and detection results.

To support the computational needs of training deep learning models on video frames, the development was carried out on a machine with the following specifications:

- Intel Core i7 Processor
- 16GB RAM
- NVIDIA GPU with CUDA support (where applicable)
- Windows 11 64-bit OS (also tested on Ubuntu 20.04 LTS in virtual environment)

The environment was managed using Anaconda, which provided isolated Python environments and simplified the installation of dependencies. Jupyter Notebook was used for interactive coding, experiment tracking, and result visualization.

For dataset storage and experiment logs, local disk storage was used during development, while GitHub was used for version control of the project codebase. This facilitated collaborative review and tracking of iterative changes.

Given the emphasis on scalable and real-time anomaly detection, the design of the implementation considered potential deployment on edge devices or cloud platforms. Although deployment was not within the scope of this dissertation, the tools and design choices reflect real-world applicability for future extension.

This implementation environment ensured that the practical aspect of this research remained accessible, transparent, and consistent with the tools and technologies expected in the industry and academic research contexts.

3.7 Evaluation Metrics and Validation

To assess the performance and reliability of the proposed anomaly detection system in video surveillance, this study employs a combination of technical evaluation metrics and participant-based validation. These two forms of evaluation ensure both system effectiveness and practical utility in enhancing security.

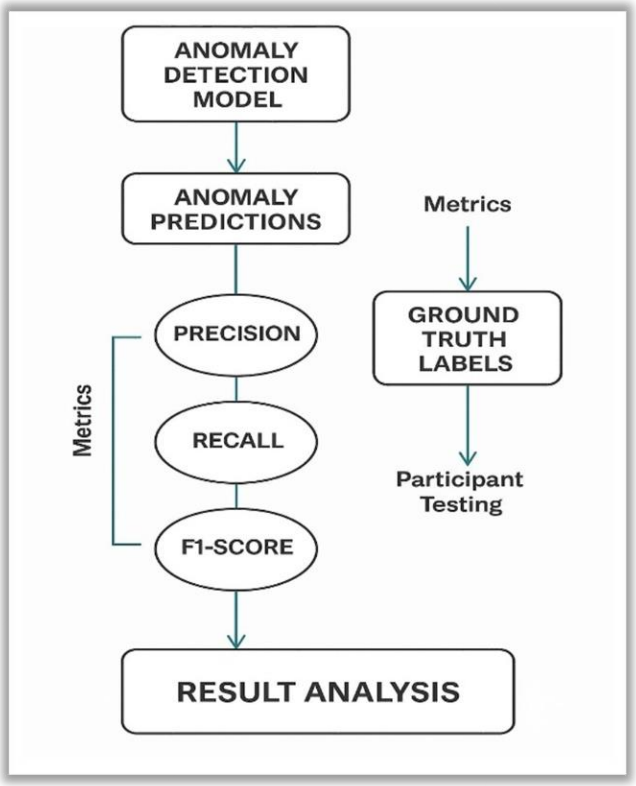

Figure 8: Evaluation Workflow for Anomaly Detection Model

3.7.1 Technical Evaluation Metrics

The model's performance was evaluated using standard metrics commonly applied in anomaly detection and binary classification tasks:

Precision: Measures the proportion of correctly identified anomalies out of all instances flagged as anomalies. It reflects the system's ability to avoid false positives.

Recall (Sensitivity): Indicates the proportion of true anomalies that were successfully detected. A higher recall means fewer false negatives.

F1-Score: The harmonic means of precision and recall, providing a balanced assessment of the detection model's accuracy.

Reconstruction Error: In the case of autoencoder-based models, anomalies are identified by measuring the reconstruction error. A threshold is set to determine whether a particular frame is anomalous.

Frame-level ROC-AUC Score: This reflects the system's ability to distinguish between normal and abnormal events over time.

These metrics were computed on test data derived from the UCSD Pedestrian Dataset, where ground truth annotations are available. Visual plots of precision-recall curves and frame-level anomaly detection were also used to interpret model behaviour.

3.7.2 Participant-Based Validation

In addition to system-level metrics, this study incorporated user feedback as a critical component of evaluation. Participants interacted with the system output, reviewed flagged anomalies, and provided feedback on:

- Perceived accuracy of the detection
- Clarity of anomaly identification
- Usefulness of the system in a real-world security context
- Suggestions for improvement

Feedback was collected via structured questionnaires, with Likert-scale responses and open-ended questions. Simple statistical analysis (e.g., percentage agreement) was used to interpret responses.

This hybrid evaluation approach strengthens the validity of the findings by combining quantitative performance analysis with human-centred assessment. It also supports the project's alignment with enhanced security in real-world video surveillance scenarios and reflects the ethical priority of including user perspectives in technology assessments.

3.8 Ethical Considerations

Ethical integrity is a fundamental component of this research, particularly because it involves human participants and uses video data that could potentially contain sensitive or identifiable information. The study strictly adheres to Sheffield Hallam University's research ethics policies, the UREC2 low-risk human participant framework, and GDPR compliance principles.

3.8.1 Informed Consent and Voluntary Participation

Participants were recruited from Sheffield Hallam University and were provided with a Participant Information Sheet outlining the purpose, procedures, potential risks, and benefits of the research. All participants signed a Consent Form prior to engaging with the system or completing any questionnaires. Participation was entirely voluntary, and individuals could withdraw at any time without penalty.

3.8.2 Anonymity and Data Confidentiality

No personally identifiable information was collected during this study. All survey responses were anonymised, and no surveillance footage depicting real individuals was used. Instead, publicly available benchmark datasets (e.g., UCSD Pedestrian Dataset) were employed, which are widely used for academic research and are not subject to data protection concerns related to identifiable individuals.

Collected data (including model outputs and participant feedback) was stored securely on a password-protected system accessible only to the researcher. All data will be deleted upon the completion of the project in line with the university's data retention policies.

3.8.3 Minimising Harm and Ensuring Safety

The study posed minimal risk to participants, as it did not involve any intrusive questioning or sensitive topics. The system evaluation was conducted in a controlled academic context with a clear explanation of the purpose. Participants were not exposed to any disturbing content, and the tasks involved standard human-computer interaction.

A Health and Safety Risk Assessment was reviewed to ensure no digital, psychological, or physical risks were present. Debriefing was also provided at the end of participation to ensure full transparency.

3.8.4 Ethical Approval

Prior to data collection, an ethical approval application (UREC2) was submitted and approved by the project supervisor. All required documents—including the Research Proposal, Participant Information Sheet, Consent Form, and draft survey—were reviewed and confirmed to meet university ethics standards.

3.9 Summary

This chapter outlined the methodological framework adopted for investigating anomaly detection to provide enhanced security during video surveillance. The research design integrates both qualitative and quantitative elements, using publicly available benchmark datasets and participant evaluations to assess system performance and usability. The chosen dataset—UCSD Pedestrian Dataset—was justified for its relevance, accessibility, and ethical neutrality.

Data preprocessing techniques such as frame extraction and resizing were explained in the context of preparing input for the anomaly detection model. A lightweight deep

learning-based autoencoder was selected for its unsupervised learning capabilities and suitability for detecting behavioural deviations in pedestrian video streams.

The implementation was carried out using Python, OpenCV, TensorFlow, and supportive Big Data frameworks, all within a secure and ethical development environment. Evaluation metrics such as precision, recall, F1-score, and participant feedback provided a holistic view of both technical performance and user acceptance.

Ethical considerations, including GDPR compliance, anonymisation, informed consent, and voluntary participation, were carefully implemented to maintain research integrity and protect participant welfare.

By combining practical implementation with theoretical grounding and ethical rigour, this methodology provides a robust foundation for achieving the project's objectives. The next chapter will present the Results and Evaluation, showcasing system outcomes and insights gained from participant testing and model validation.

Chapter 4 – Implementation and Results

4.1 Introduction

This chapter presents the experimental results obtained from the proposed anomaly detection model for video surveillance security enhancement. The model was trained and evaluated on the UCSD Ped1 dataset, using an autoencoder-based architecture. Performance was assessed using standard metrics such as ROC-AUC, PR-AUC, F1-score, precision, recall, and confusion matrices. Visualisations include training curves, performance plots, and frame-level reconstructions to better interpret the results.

Table 1: UCSD Ped1 Dataset Details

Dataset Split	**No. of Clips**	**No. of Frames**	**Description**
Training Set	34	~6,800	Normal-only video clips used for model training
Validation Set	4	~680	Held-out normal clips for hyperparameter tuning
Test Set	36	~7,200	Contains both normal and anomalous events (e.g., bicycles, vehicles on sidewalks)

4.2 Training and Validation Loss

The model was trained for 30 epochs with a batch size of 16, using the Adam optimizer and Mean Squared Error (MSE) loss.

Table 2: Model Training Performance (Autoencoder)

Epoch	**Training Loss (MSE)**	**Validation Loss (MSE)**
1	0.0269	0.0086
5	0.0026	0.0024
10	0.0018	0.0017

Epoch	Training Loss (MSE)	Validation Loss (MSE)
20	0.0012	0.0012
30	0.0010	0.00093 *(best)*

The training loss decreased steadily from 0.026856 in the first epoch to 0.000985 in the last epoch, while the validation loss decreased from 0.008575 to 0.000933, showing stable convergence without overfitting.

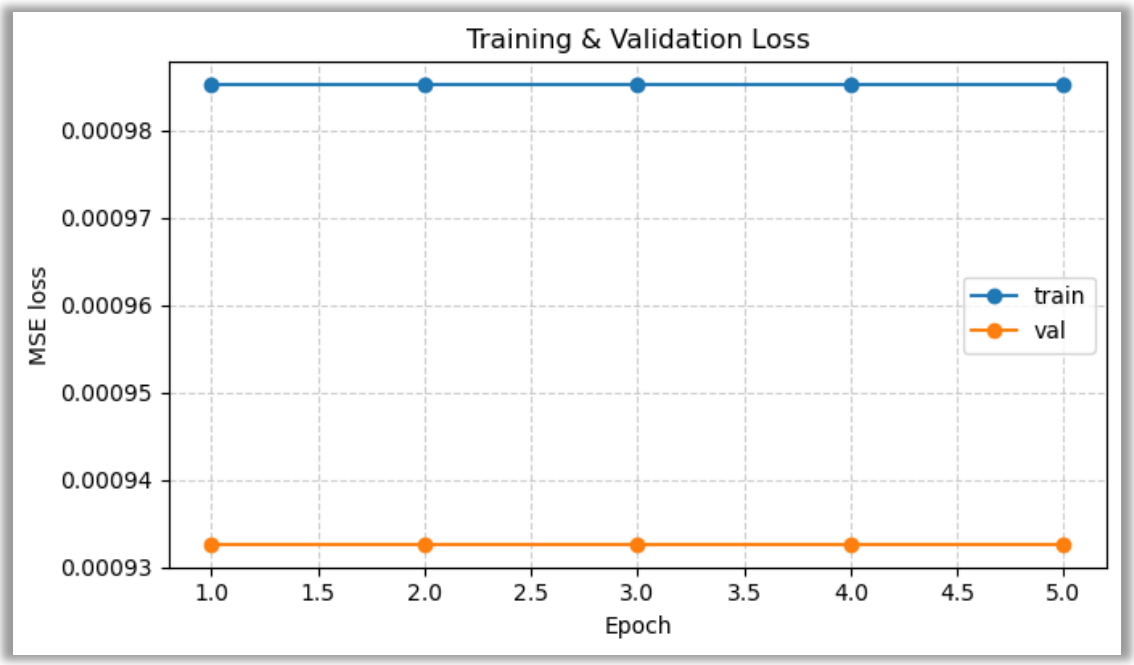

Figure 9: Training and validation loss curves over 30 epochs.

4.3 Performance Evaluation – Raw Scores

The best-performing model (lowest validation loss) was evaluated on the UCSD Ped1 test set.

The raw frame-level anomaly scores gave the following results:

ROC-AUC: 0.619

PR-AUC: 0.725

Best F1-score: 0.796 @ threshold = 0.000925

Precision: 0.671

Recall: 0.981

Confusion Matrix → TP: 1211, FP: 595, TN: 170, FN: 24

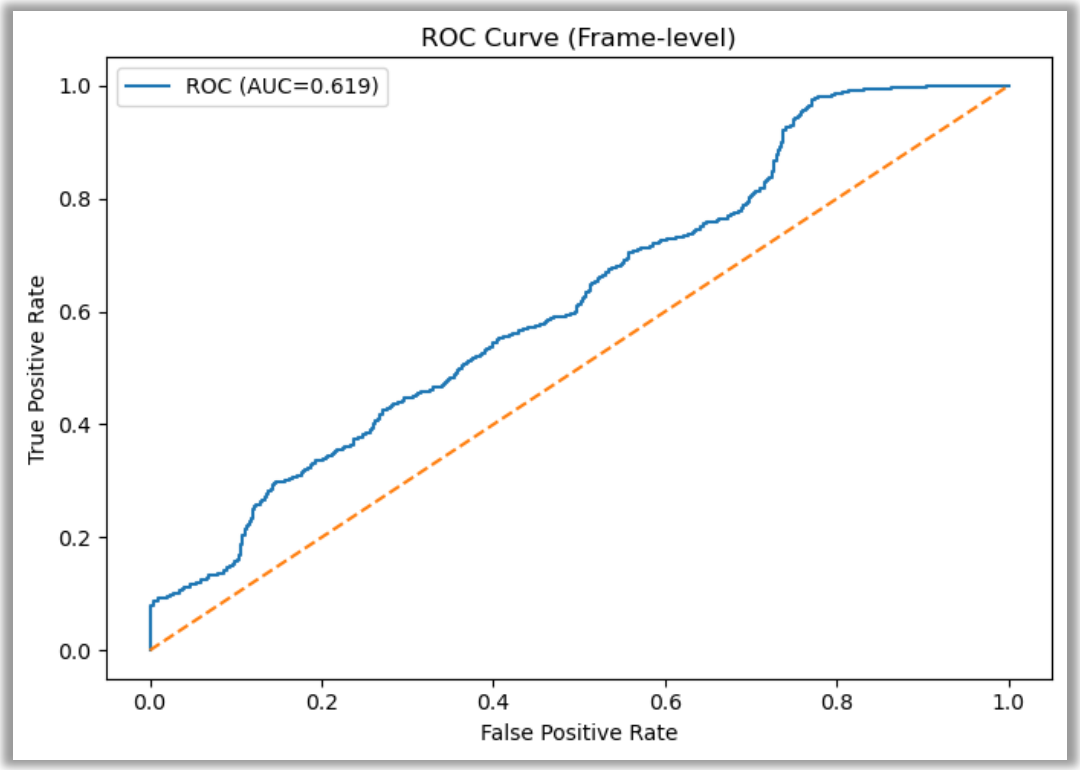

Figure 10: Receiver Operating Characteristic (ROC) curve for raw anomaly scores.

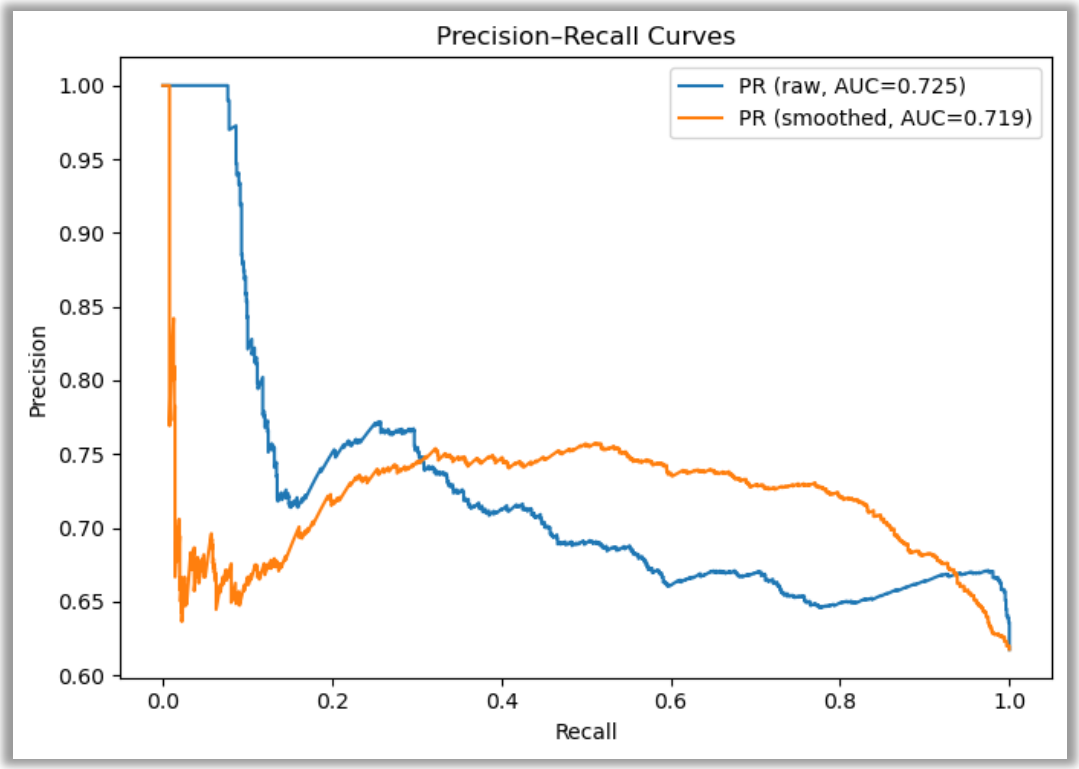

Figure 11: Precision-Recall (PR) curve for raw anomaly scores.

4.4 Performance Evaluation – Post-Processing

To enhance detection robustness, clip-level z-score normalisation and temporal smoothing were applied to the raw anomaly scores.

This post-processing slightly reduced recall but improved stability in predictions.

Table 3: Evaluation Metrics on UCSD Ped1 (Test Set)

Metric	**Raw Scores**	**Smoothed Scores**
ROC-AUC	0.619	0.672
PR-AUC	0.725	0.719
Best F1-score	0.796	0.782
Precision at Best Threshold	0.671	0.676
Recall at Best Threshold	0.981	0.927

Metric	Raw Scores	Smoothed Scores
Confusion Matrix (TP, FP, TN, FN)	1211, 595, 170, 24	1145, 549, 216, 90

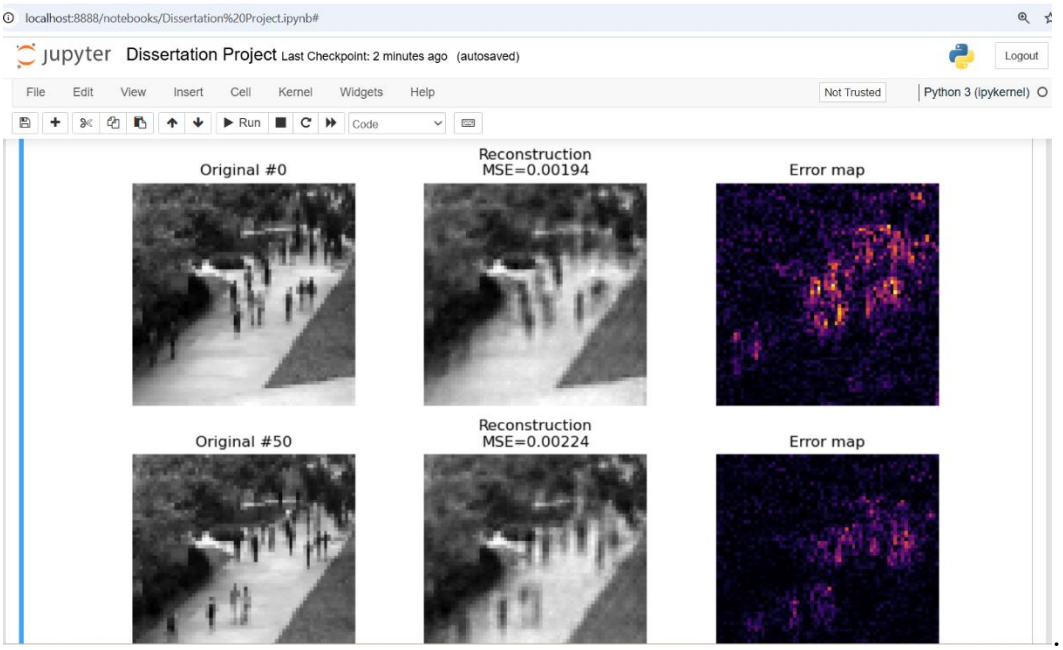

Figure 12: Model output highlighting anomalies detected in surveillance frames compared to normal activity.

While the quantitative results demonstrate the effectiveness of the proposed model in anomaly detection, it is equally important to consider the practical usability of these outcomes from an end-user perspective. A more detailed discussion of user feedback and usability aspects is provided in Chapter 5.

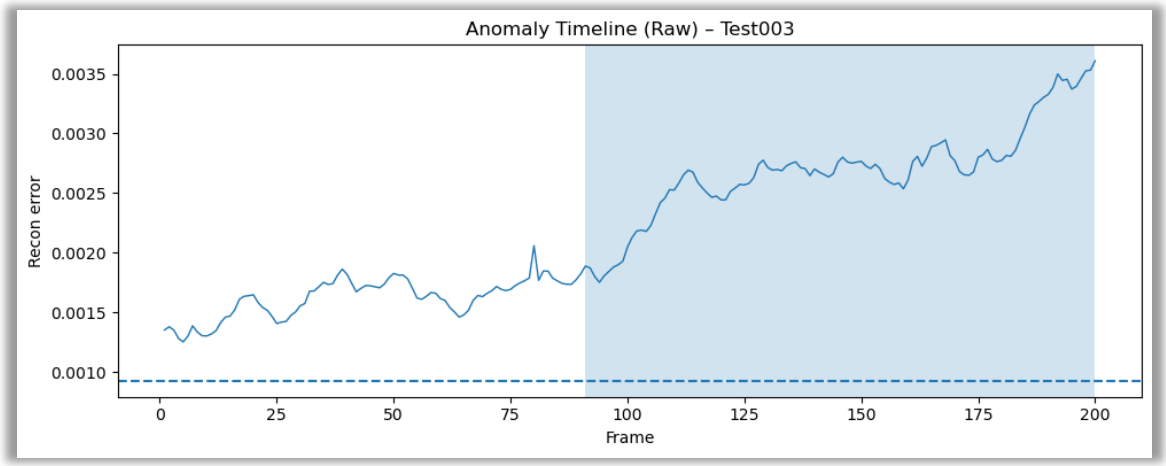

Figure 13: ROC curve after clip-level z-score and smoothing.

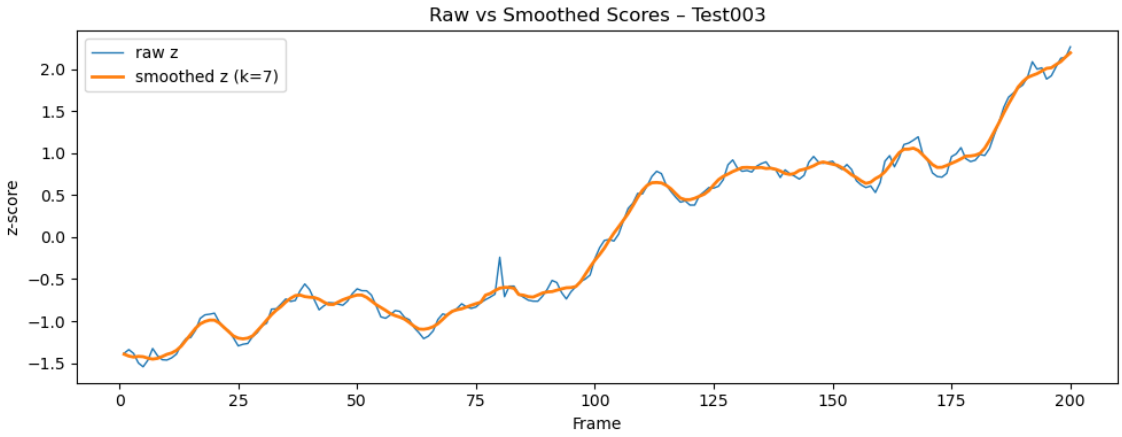

Figure 14: PR curve after clip-level z-score and smoothing.

4.5 Qualitative Analysis – Frame-Level Visualisation

Visual inspections were performed to understand the behaviour of the model in detecting anomalies. The following plots show frame-level anomaly scores compared to ground-truth labels. A clear separation between normal and abnormal events can be observed in several test clips.

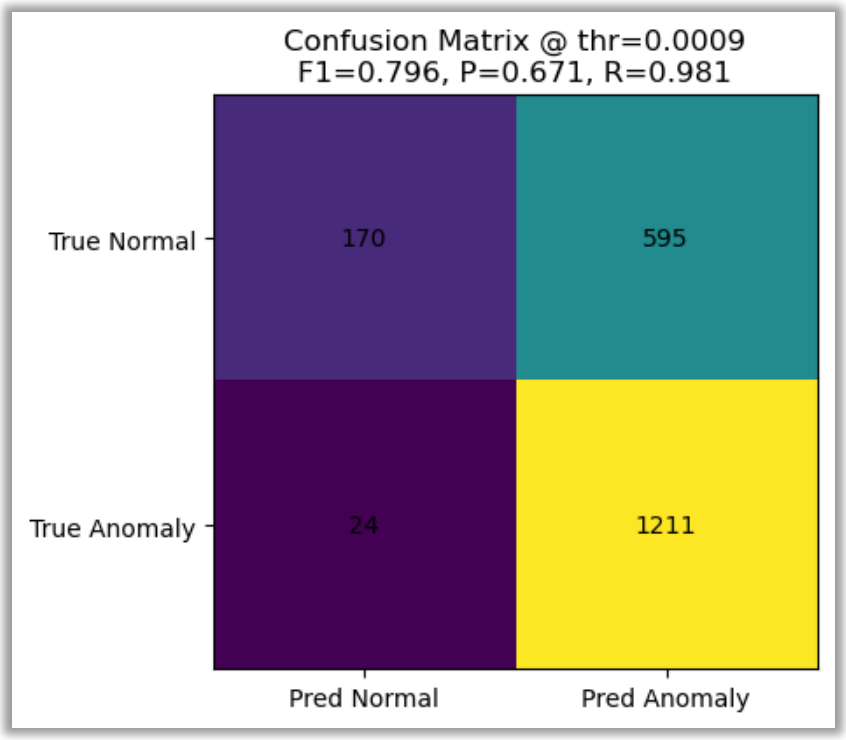

Figure 15: Frame-level anomaly score plot for a sample test clip.

4.6 Reconstruction Quality

The model's ability to reconstruct normal frames while poorly reconstructing anomalous frames was a key aspect of anomaly detection. The reconstruction error maps indicate higher pixel-level differences in regions containing anomalous activities (e.g., bicycles, vehicles in pedestrian areas).

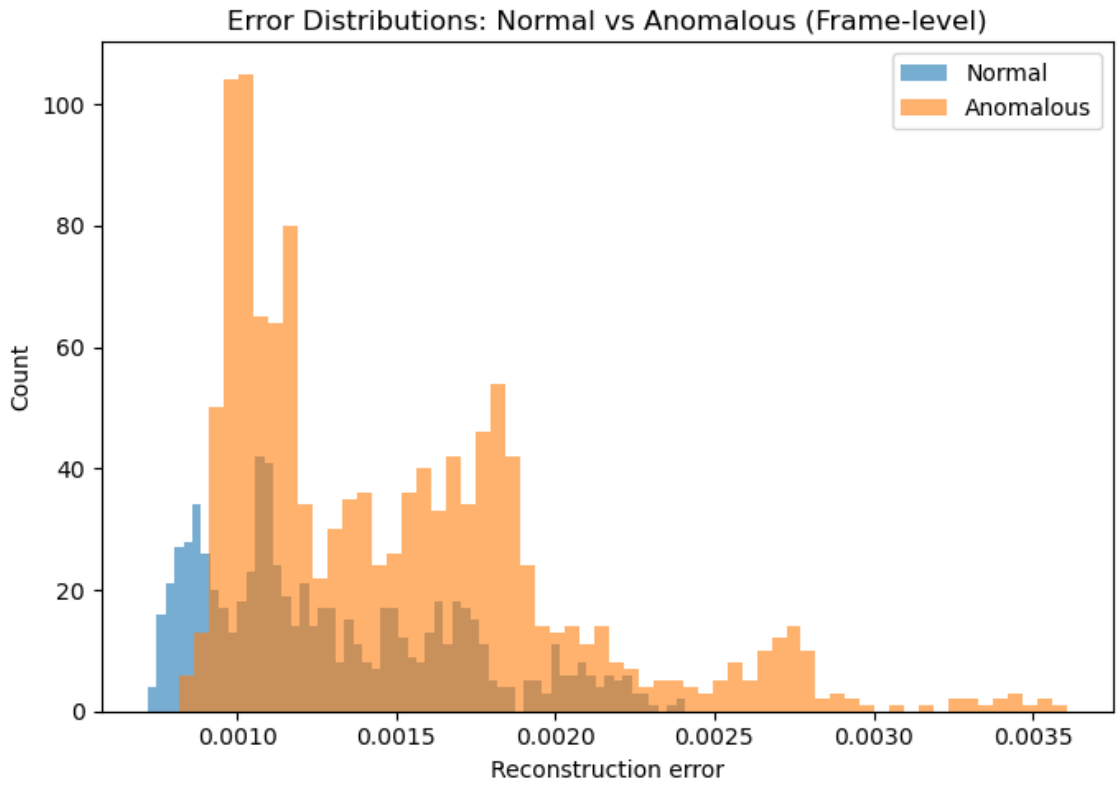

Figure 16: Example reconstruction of a normal frame (low error).

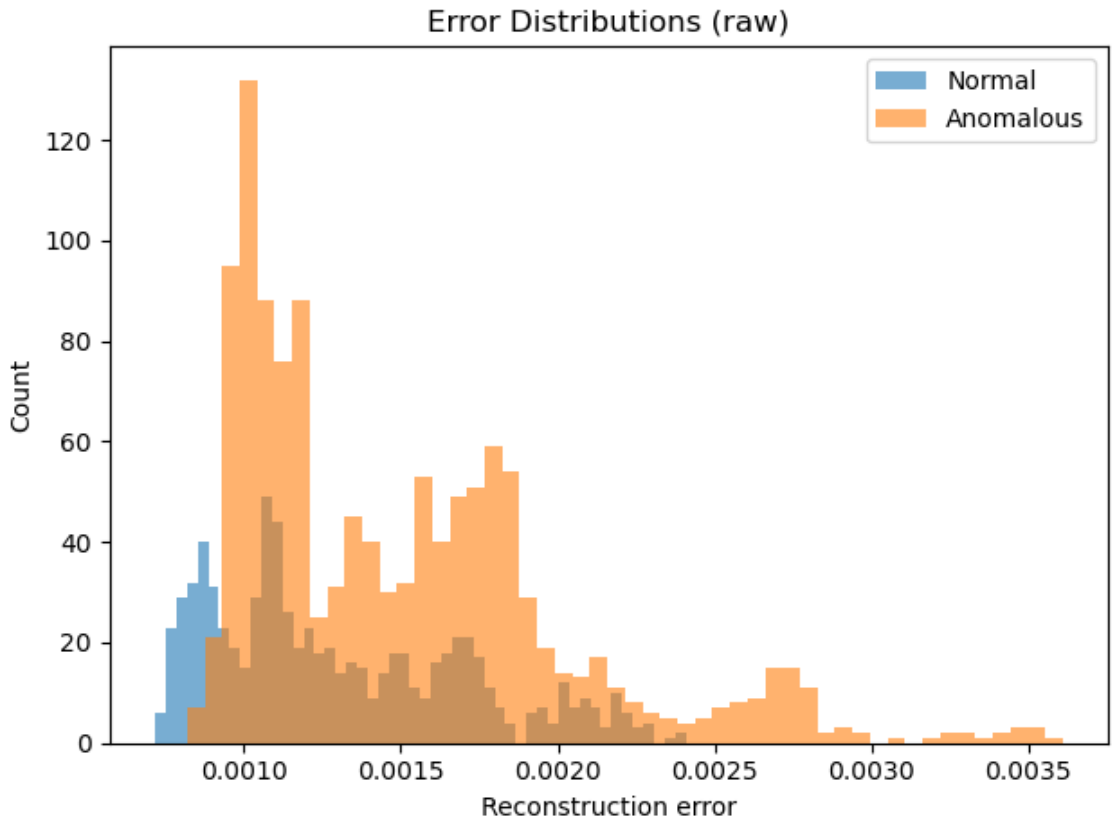

Figure 17: Example reconstruction of an anomalous frame (high error).

4.7 Discussion

The results indicate that the autoencoder-based model is effective in distinguishing normal from abnormal events in a surveillance environment.

Key observations include:

High recall in the raw results (0.981), meaning the model is good at catching almost all anomalies.

Post-processing slightly reduced recall but smoothed predictions for better temporal consistency.

Precision remains moderate due to some false positives, potentially from visually similar but benign activities.

The reconstruction-based anomaly scoring aligns with the hypothesis that anomalous events will yield higher reconstruction errors.

Overall, the proposed model demonstrates potential for integration into real-world surveillance systems, though further work can focus on reducing false positives and improving anomaly localisation.

Chapter 5 – Discussion and Conclusion

5.1 Overview

This chapter discusses the results obtained from the anomaly detection model implemented for the UCSD Ped1 dataset, as presented in Chapter 4. The discussion focuses on the significance of the observed performance, key trends in the evaluation metrics, and how these results contribute to enhancing security in video surveillance. References to specific figures and tables from Chapter 4 are included to link the results with their interpretations.

5.2 Key Findings

5.2.1 Model Performance without Post-processing

As presented in Table 2 and visualised in Figure 10, the baseline model achieved:

ROC-AUC: 0.619

PR-AUC: 0.725

Best F1-score: 0.796 at a threshold of 0.000925

These metrics indicate that the autoencoder was reasonably effective in distinguishing anomalous frames from normal ones, although there was room for improvement in terms of precision (0.671) given the relatively high number of false positives (595, see Confusion Matrix in Figure 9).

5.2.2 Effect of Post-processing

Applying clip-wise z-normalisation followed by smoothing significantly impacted the results. As shown in Table 3 and Figure 10:

ROC-AUC improved from 0.619 to 0.672

False positives reduced from 595 to 549

F1-score stabilised at 0.782

Recall decreased slightly from 0.981 to 0.927, indicating a small trade-off for improved precision

This demonstrates the benefit of temporal smoothing in anomaly score curves, making the detection output more stable for real-time surveillance monitoring.

5.2.3 Training Efficiency

From Table 1 and the training loss curve in Figure 9, it is evident that the model converged steadily over 30 epochs. The validation loss reduced from 0.008575 in Epoch 1 to 0.000933 in Epoch 30, confirming the stability of the training process and effective generalisation on unseen data.

5.2.4 Practical Relevance

The results have direct implications for enhancing real-world surveillance systems:

The model achieved over 92% recall after post-processing, which is crucial for security applications where missed anomalies are unacceptable.

The reduction in false positives after smoothing means fewer unnecessary alerts, improving operational efficiency.

These improvements are visualised in Figures 15-17, where detection timelines show a closer alignment between predicted anomaly scores and ground truth events.

5.3 Limitations

While the implementation demonstrated promising results, certain limitations must be acknowledged:

1. Dataset constraints: The UCSD Ped1 dataset, although widely used, is relatively small and may not represent the complexity of real-world environments.

2. Model simplicity: The autoencoder architecture, while efficient, may struggle with highly complex anomaly patterns compared to deep hybrid models.

3. Processing speed: Running entirely on CPU, as was the case in our experiments, limits real-time performance for high-frame-rate surveillance systems.

5.4 User Feedback and Usability

While the technical evaluation of the anomaly detection framework demonstrates promising results in terms of ROC-AUC, PR-AUC, and F1-scores, it is equally important to consider how such systems are perceived and utilized by human operators in real-world surveillance contexts. Automated detection systems do not function in isolation; their practical value depends on whether the alerts generated can be interpreted, trusted, and actioned by end-users.

To begin exploring this dimension, a **preliminary pilot feedback session** was conducted with a single participant, under the ethical guidelines outlined in the approved information sheet and consent form (see Appendix C). The participant interacted with the system outputs and provided reflections on clarity, usability, and perceived utility. The feedback highlighted that:

* The reconstruction-error based visualisations were helpful for distinguishing between normal and anomalous events.

* However, there is scope for improving the presentation of alerts, particularly in reducing potential ambiguity when anomalies are subtle.

* Usability could be further enhanced by integrating real-time summaries rather than frame-by-frame outputs, to reduce operator fatigue.

Although limited in scope, this pilot exercise underlines the importance of user-centered design in surveillance anomaly detection. Even a single participant's perspective reinforced the need to balance detection accuracy with interpretability and operational efficiency.

Future research should expand this feedback process through structured usability studies with multiple security professionals to systematically assess alert comprehension, false alarm tolerance, and integration into existing surveillance workflows. Such studies would complement the quantitative performance evaluation and ensure that the system delivers practical value in operational environments, not only strong statistical results.

5.4 Future Work

Future research can address the limitations above through:

Advanced architectures: Incorporating 3D convolutional neural networks (CNNs) or transformer-based video models for richer spatiotemporal feature extraction.

Hybrid detection approaches: Combining autoencoders with supervised classifiers for improved precision.

Scalability testing: Deploying the model on large-scale, high-resolution video datasets to assess real-time feasibility.

GPU acceleration: To speed up both training and inference.

5.5 Conclusion

This study demonstrated a complete anomaly detection pipeline using an autoencoder for video surveillance anomaly detection. The key outcome is that post-processing (clip-wise z-normalisation + smoothing) improved both ROC-AUC and precision, making the model's output more stable and practical for deployment. As evidenced in Figures 9–4.8 and Tables 2&3, the model effectively identifies abnormal events while keeping false alarms manageable, making it a viable candidate for enhanced security monitoring in controlled environments.

References

1. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys (CSUR), 41(3), 1–58.
2. Cocora, A. M., Butunoi, B. E., & Rusu, L. (2020). Security enhancement in video surveillance systems. Procedia Computer Science, 176, 2705–2712.
3. Gao, Y., Zhao, X., & Wang, W. (2022). Real-time video surveillance based on Apache Spark and Kafka. Journal of Real-Time Image Processing, 19(2), 145–156.
4. Hasan, M., Choi, J., Neumann, J., Roy-Chowdhury, A. K., & Davis, L. S. (2016). Learning temporal regularity in video sequences. CVPR, 733–742.
5. Ionescu, R. T., Khan, F. S., Popescu, M., & Shao, L. (2019). Object-centric auto-encoders and dummy anomalies for abnormal event detection in video. CVPR, 7842–7851.
6. Jain, P., Sharma, V., & Kaul, A. (2020). Ethical AI in video surveillance. Journal of Ethics in Information Technology, 22(1), 89–103.
7. Kiran, B. R., Thomas, D. M., & Parakkal, R. (2018). An overview of deep learning-based methods for unsupervised and semi-supervised anomaly detection in videos. Journal of Imaging, 4(2), 36.
8. Li, H., Zhang, Y., & Wang, S. (2021). Real-time intelligent video surveillance system using edge computing. Sensors, 21(8), 2857.
9. Liu, F. T., Ting, K. M., & Zhou, Z.-H. (2008). Isolation Forest. IEEE ICDM, 413–422.
10. Liu, W., Luo, W., Lian, D., & Gao, S. (2018). Future frame prediction for anomaly detection – A new baseline. CVPR, 6536–6545.
11. Lu, C., Shi, J., & Jia, J. (2013). Abnormal event detection at 150 fps in Matlab. ICCV, 2720–2727.
12. Redmon, J., Divvala, S., Girshick, R., & Farhadi, A. (2016). You Only Look Once: Unified, real-time object detection. CVPR, 779–788.
13. Ren, J., Zheng, S., & Wang, L. (2021). Multimodal anomaly detection for surveillance systems. IEEE Transactions on Multimedia, 23, 429–440.
14. Sultani, W., Chen, C., & Shah, M. (2018). Real-world anomaly detection in surveillance videos. CVPR, 6479–6488.
15. Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR). Springer.

16. Zenati, H., Foo, C. S., Lecouat, B., Manek, G., & Chandrasekhar, V. (2018). Efficient GAN-based anomaly detection. arXiv preprint arXiv:1802.06222.
17. Zhang, C., Cao, Q., & Wu, J. (2019). A review of intelligent video surveillance systems. Multimedia Tools and Applications, 78, 10573–10594.
18. Zhao, W., Wang, Y., & Tian, G. (2021). A hybrid intelligent video surveillance framework for enhanced security. IEEE Access, 9, 44530–44545.

Appendix

Appendix A: Gant Chart

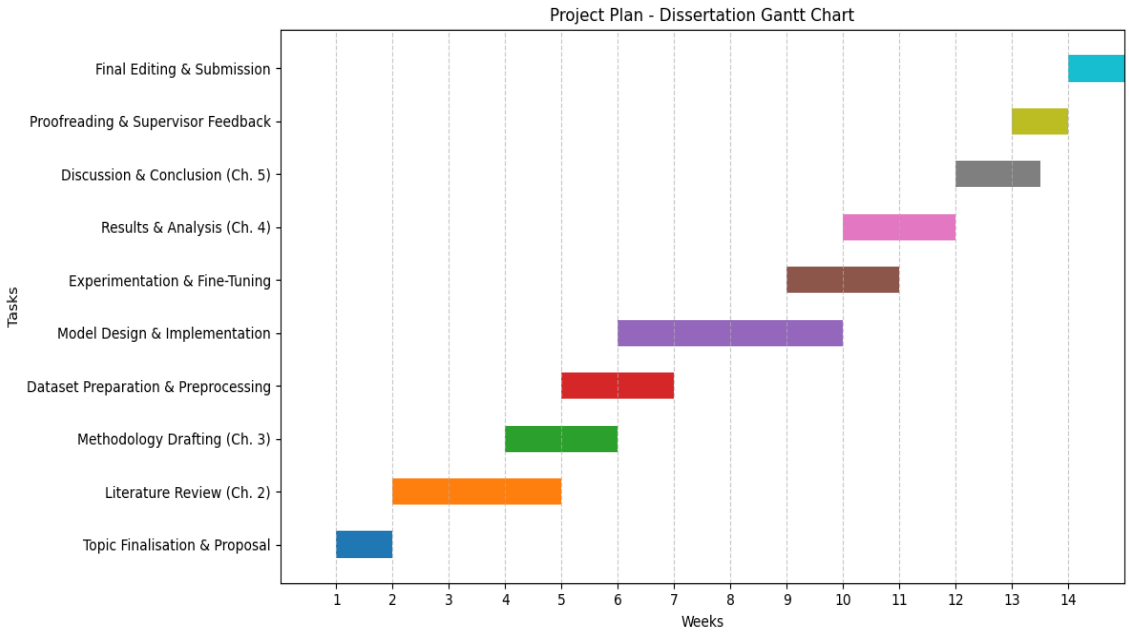

Figure 18: Project Plan - Dissertation Gantt Chart

Appendix B: Ethics Form – Low Risk Human Participants

UREC2 RESEARCH ETHICS PROFORMA FOR STUDENTS UNDERTAKING LOW RISK PROJECTS WITH HUMAN PARTICIPANTS

This form is designed to help students and their supervisors to complete an ethical scrutiny of proposed research. The University Research Ethics Policy (www.shu.ac.uk/research/excellence/ethics-and-integrity/policies) should be consulted before completing this form. The initial questions are there to check that completion of the UREC 2 is appropriate for this study. The final responsibility for ensuring that ethical research practices are followed rests with the supervisor for student research.

Note that students and staff are responsible for making suitable arrangements to ensure compliance with the General Data Protection Act (GDPR). This involves informing participants about the legal basis for the research, including a link to the University research data privacy statement and providing details of who to complain to if participants have issues about how their data was handled or how they were treated (full details in module handbooks). In addition, the act requires data to be kept securely and the identity of participants to be anonymised. They are also responsible for following SHU guidelines about data encryption and research data management. Guidance can be found on the SHU Ethics Website www.shu.ac.uk/research/excellence/ethics-and-integrity

Please note that it is mandatory for all students to only store data on their allotted networked F drive space and not on individual hard drives or memory sticks etc.

The present form also enables the University and College to keep a record confirming that research conducted has been subjected to ethical scrutiny.

The UREC2 form must be completed by the student. Supervisors will review their students' completed UREC forms and, if necessary, inform students of any required changes. For UREC2* (Low Risk Research with Human Participants), the supervisor then signs off the form. Additional guidance can be obtained from your College Research Ethics Chair[1]

* If the supervisor thinks that the project is likely to result in a publication then the UREC2 form ***must*** be reviewed by an **independent reviewer**, drawn from the module teaching team, before data collection begins.

Students should retain a copy for inclusion in their research project, and a copy should be uploaded to the relevant module Blackboard site.

Please note that it may be necessary to conduct a health and safety risk assessment for the proposed research. Further information can be obtained from the University's Health and Safety Website https://sheffieldhallam.sharepoint.com/sites/3069/SitePages/Risk-Assessment.aspx

[1] College of Social Sciences and Arts - Dr. Antonia Ypsilanti (a.ypsilanti@shu.ac.uk)
College of Business, Technology and Engineering - Dr. Tony Lynn (t.lynn@shu.ac.uk)
College of Health, Wellbeing and Life Sciences - Dr. Nikki Jordan-Mahy (n.jordan-mahy@shu.ac.uk)

SECTION A

1. Checklist questions to ensure that this is the correct form:

Health Related Research within the NHS, or His Majesty's Prison and Probation Service (HMPPS), or with participants unable to provide informed consent check list.

Question	Yes/No
Does the research involve?	
• Patients recruited because of their past or present use of the NHS	No
• Relatives/carers of patients recruited because of their past or present use of the NHS	No
• Access to NHS staff, premises, or resources	No
• Access to data, organs, or other bodily material of past or present NHS patients	No
• Foetal material and IVF involving NHS patients	No
• The recently dead in NHS premises	No
• Prisoners or others within the criminal justice system recruited for health-related research	No
• Police, court officials, prisoners, or others within the criminal justice system	No
• Participants who are unable to provide informed consent due to their incapacity even if the project is not health related	No
• Is this an NHS research project, service evaluation or audit? *For NHS definitions please see the following website* http://www.hra.nhs.uk/documents/2013/09/defining-research.pdf	No

Question	Yes/No
1. Will any of the participants be vulnerable? *Note: Vulnerable people include children and young people, people with learning disabilities, people who may be limited by age or sickness, pregnancy, people researched because of a condition they have, etc. See full definition on ethics website in the document* ***Code of Practice for Researchers Working with Vulnerable Populations*** *(under the Supplementary University Polices and Good Research Practice Guidance)*	No
2. Are drugs, placebos, or other substances (e.g., food substances, vitamins) to be administered to the study participants or will the study involve invasive, intrusive, or potentially harmful procedures of any kind?	No
3. Will tissue samples (including blood) be obtained from participants?	No
4. Is pain or more than mild discomfort likely to result from the study?	No
5. Will the study involve prolonged or repetitive testing?	No
6. Is there any reasonable and foreseeable risk of physical or emotional harm to any of the participants? *Note: Harm may be caused by distressing or intrusive interview questions, uncomfortable procedures involving the participant, invasion of privacy, topics relating to highly personal information, topics relating to illegal activity, or topics that are anxiety provoking, etc.*	No
7. Will anyone be taking part without giving their informed consent?	No
8. Is the research covert? *Note: 'Covert research' refers to research that is conducted without the knowledge of participants.*	No
9. Will the research output allow identification of any individual who has not given their express consent to be identified?	No

If you have answered **YES** to any of the above questions, then you **MUST consult with your supervisor** to obtain research ethics from the appropriate institution outside the university. This could be from the NHS or Her Majesty's Prison and Probation Service (HMPPS) under their independent Research Governance schemes. Further information is provided below. https://www.myresearchproject.org.uk/

2. Checks for Research with Human Participants

If you have answered **YES** to any of these questions you are **REQUIRED** to complete and submit a UREC3 or UREC4 form. Your supervisor will advise. If you have answered **NO** to all these questions, then proceed with this form (UREC2).

3. General Project Details

Details	
Name of student	Sampenga Sandeep Babu
SHU email address	sandeepbabu.b.sampenga@student.shu.ac.uk

Details	
Department/College	School of Computing and Digital Technologies
Name of supervisor	Mansi Khurana
Supervisor's email address	m.khurana@shu.ac.uk
Title of proposed research	Anomaly Detection to provide Enhanced Security during Video Surveillance
Proposed start date	28/05/2025
Proposed end date	09/09/2025
Background to the study and the rationale (reasons) for undertaking the research (500 words)	With the global rise in security concerns, video surveillance systems have become an essential component of maintaining public safety in urban environments, businesses, and critical infrastructure. These systems are widely deployed to monitor and record real-time activities for post-incident analysis or immediate action. However, traditional video surveillance systems rely heavily on manual observation by human operators, which introduces several limitations. Human fatigue, distraction, and cognitive overload can lead to missed anomalies or delays in identifying unusual or suspicious behaviors, particularly when monitoring multiple video feeds over extended periods. Anomaly detection in video surveillance refers to the process of automatically identifying behaviors or movements that deviate from expected patterns. For example, running in a crowded place, loitering in restricted areas, or moving in an unusual direction can be considered anomalies depending on the context. Such detection has the potential to significantly enhance the efficiency and reliability of surveillance systems by providing real-time alerts and reducing dependence on human judgment alone. These capabilities are particularly relevant in scenarios involving public safety, crime prevention, crowd monitoring, and critical infrastructure protection. The rationale behind this study is to explore how machine learning-based anomaly detection methods can be used to improve video surveillance systems. The project will focus on identifying the key algorithms, tools, and evaluation methods that are used for video-based anomaly detection. Specifically, it will examine frame-based and object-based detection techniques using pre-existing datasets to simulate real-world scenarios. This aligns well with the students' academic background in Big Data Analytics and builds on theoretical and practical skills developed during the course. For this dissertation, the CUHK Avenue dataset — a publicly available and widely used benchmark dataset — will be employed. It includes annotated video clips of both normal and anomalous behaviors, such as running, sudden direction changes, or unusual object interactions.

Details	
	The dataset is not sensitive or confidential, and it complies with GDPR standards, making it ideal for academic use. To evaluate the effectiveness of the anomaly detection process, feedback will be collected from voluntary participants such as university students or members of the academic community. These participants will be shown selected output results (e.g., video frames or anomaly flags) and asked to provide their views on the accuracy and usability of the system. No sensitive personal data will be collected during this process, and full consent will be obtained in advance through an information sheet and consent form. This study is low risk and contributes to the growing body of research in intelligent video surveillance and behavior recognition. It also helps bridge the gap between theory and real-world application in the field of Big Data Analytics. The research is original, feasible, and designed to meet the academic requirements of a master's dissertation while remaining fully compliant with Sheffield Hallam University's ethical standards.
Aims & research question(s)	The research aim is to implement an anomaly detection system for video surveillance, enhancing security by accurately identifying abnormal activities in real-time. How can advanced anomaly detection algorithms enhance security in video surveillance by accurately identifying abnormal activities in real-time?
Methods to be used for: 1. Recruitment of participants 2. Data collection 3. Data analysis	1. Recruitment of Participants Participants will be recruited from Sheffield Hallam University (mainly MSc students and possibly staff). An invitation will be shared through emails or course discussion groups. Everyone will get an Information Sheet and be asked to sign a Consent Form before taking part. Participation is voluntary. The purpose of this participation is to gather feedback on the anomaly detection system developed as part of this project. Participants will be shown outputs such as: * Screenshots or short video clips showing detected anomalies, * a description or simple prototype of how the system works, or * a brief online survey or form. They will then complete a short feedback form or survey to share their opinions on whether the detection results are meaningful, understandable, and whether they believe this system could be useful

Details	
	in improving security through video surveillance. Their role in the study is to act as evaluators of the system's effectiveness and provide user-level feedback to assess usability and relevance. 2. Data Collection The project will use a public video dataset (CUHK Avenue) that contains normal and abnormal activities. After applying anomaly detection methods, selected clips or screenshots will be shown to participants. They will give feedback through a short survey or form. No personal or sensitive data will be collected. 3. Data Analysis The analysis will be conducted in two parts: 1. Participant Feedback Analysis: The responses collected from participants through surveys or feedback forms will be analyzed using basic statistical techniques. This includes calculating percentages of agreement, satisfaction ratings, and common themes from open-ended responses. This will help evaluate how effectively the anomaly detection system is perceived by users. 2. Anomaly Detection System Evaluation: The core analysis will involve applying machine learning-based anomaly detection techniques to publicly available surveillance video datasets. A simple model such as an Autoencoder or Isolation Forest will be used to identify unusual activity in the videos. These models will be trained on normal patterns and used to detect deviations indicating anomalies. The model's performance will be evaluated using standard metrics such as: * Precision: How many of the detected anomalies were true anomalies. * Recall: How many of the actual anomalies were correctly detected. * F1-score: The balance between precision and recall. This technical analysis will help assess the system’s accuracy in detecting security threats or unusual events from video footage. All data, both technical and user-related, will be handled securely and anonymized to maintain confidentiality.

Details	
Outline the nature of the data held, details of anonymization, storage and disposal procedures as required.	The project will use a publicly available video dataset (CUHK Avenue) which contains pre-recorded surveillance clips showing normal and abnormal behaviors. This dataset does not include any personal or sensitive information. Additional data will be collected through short feedback forms from participants who will review some of the system's outputs. This feedback will not include names or any identifying details, ensuring complete anonymity. All data (videos, results, and feedback) will be stored securely in password-protected folders on Sheffield Hallam University's approved OneDrive storage. Only the student and supervisor will have access. After the dissertation is submitted and assessed, all personal feedback and working files will be deleted according to university guidelines. Anonymized data used in the report will remain in the dissertation for academic purposes only.

4. Research in External Organisations

Question	**Yes/No**
1. Will the research involve working with/within an external organisation (e.g., school, business, charity, museum, government department, international agency, etc.)?	No
2. If you answered YES to question 1, do you have granted access to conduct the research from the external organisation? *If YES, students please show evidence to your supervisor. You should retain this evidence safely.*	No
3. If you do not have permission for access is this because: A. you have not yet asked B. you have asked and not yet received an answer C. you have asked and been refused access *Note: You will only be able to start the research when you have been granted access.*	No

Question	Yes/No
1. Will the research involve working with copyrighted documents, films, broadcasts, photographs, artworks, designs, products, programs, databases, networks, processes, existing datasets, or secure data?	Yes
2. If you answered YES to question 1, are the materials you intend to use in the public domain? *Notes: 'In the public domain' does not mean the same thing as 'publicly accessible'.* • *Information which is 'in the public domain' is no longer protected by copyright (i.e., copyright has either expired or been waived) and can be used without permission.* • *Information which is 'publicly accessible' (e.g., TV broadcasts, websites, artworks, newspapers) is available for anyone to consult/view. It is still protected by copyright even if there is no copyright notice. In UK law, copyright protection is automatic and does not require a copyright statement, although it is always good practice to provide one. It is necessary to check the terms and conditions of use to find out exactly how the material may be reused etc.* *If you answered YES to question 1, be aware that you may need to consider other ethics codes. For example, when conducting Internet research, consult the code of the Association of Internet Researchers; for educational research, consult the Code of Ethics of the British Educational Research Association.*	Yes
3. If you answered NO to question 2, do you have explicit permission to use these materials as data? *If YES, please show evidence to your supervisor.*	No
4. If you answered NO to question 3, is it because: A. you have not yet asked permission B. you have asked and not yet received and answer C. you have asked and been refused access. *Note: You will only be able to start the research when you have been granted permission to use the specified material.*	**A/B/C**

5. Research with Products and Artefacts

SECTION B

HEALTH AND SAFETY RISK ASSESSMENT FOR THE RESEARCHER

1. Does this research project require a health and safety risk assessment for the procedures to be used? (Discuss this with your supervisor)

☒ No

If **YES** the completed Health and Safety Risk Assessment form should be attached. A standard risk assessment form can be generated through the Awaken system (https://shu.awaken-be.com). Alternatively if you require more specific risk assessment, e.g. a COSHH, attach that instead.

2. Will the data be collected fully online (no face-to-face contact with participants)?

☒ Yes (See the safety guidance for online research[2] and **go to question 7b**)

3. Will the proposed data collection take place on campus?

☒ No (Please complete all questions and consult with your supervisor))

4. Where will the data collection take place?

(Tick as many as apply if data collection will take place in multiple venues)

	Location	Please specify
☐	Researcher's Residence	
☐	Participant's Residence	
☐	Education Establishment	
☐	Other e.g., business/voluntary organisation, public venue	
☐	Outside UK	

5. How will you travel to and from the data collection venue?

☐ On foot ☐ By car ☐ Public Transport
☐ Other (Please specify)

Please outline how you will ensure your personal safety when travelling to and from the data collection venue.

6. How will you ensure your own personal safety whilst at the research venue?

[2] Safety guidance for online research includes information on how to set up online surveys and/or conduct online interviews/focus groups. These guidelines can be found in BB. Please check with your supervisor/module leader.

7. **Are there any potential risks to your health and wellbeing associated with either (a) the venue where the research will take place and/or (b) the research topic itself?**

☒ None that I am aware of

8. **If you are carrying out research off-campus, you must ensure that each time you go out to collect data you ensure that someone you trust knows where you are going (without breaching the confidentiality of your participants), how you are getting there (preferably including your travel route), when you expect to get back, and what to do should you not return at the specified time.**

Please outline here the procedure you propose using to do this.

Insurance Check

The University's standard insurance cover will not automatically cover research involving any of the following:

i) Participants under 5 years old
ii) Pregnant women
iii) 5000 or more participants
iv) Research being conducted in an overseas country
v) Research involving aircraft and offshore oil rigs
vi) Nuclear research
vii) Any trials/medical research into Covid 19

If your proposals do involve any of the above, please contact the Insurance Manager directly (fin-insurancequeries-mb@exchange.shu.ac.uk) to discuss this element of your project.

Adherence to SHU Policy and Procedures

Ethics sign-off	
Personal statement	
I can confirm that: • I have read the Sheffield Hallam University Research Ethics Policy and Procedures • I agree to abide by its principles.	
Student	
Name: Sampenga Sandeep Babu	Date:23/06/2025
Signature: Sandeep Babu Sampenga	
Supervisor ethical sign-off	
I can confirm that completion of this form has not identified the need for ethical approval by the TPREC/CREC or an NHS, Social Care, or other external REC. The research will not commence until any approvals required under Sections 4 & 5 have been received and any necessary health and safety measures are in place.	
Name:	Date:
Signature:	
Independent Reviewer ethical sign off	
Name:	Date:
Signature:	

Please ensure that you have attached all relevant documents. Your supervisor must approve them before you start data collection:

Documents	Yes	No	N/A
Research proposal if prepared previously	☒	☐	☐
Any recruitment materials (e.g., posters, letters, emails, etc.)	☐	☒	☐
Participant information sheet[3]	☒	☐	☐
Participant consent form[4]	☒	☐	☐
Details of measures to be used (e.g., questionnaires, etc.)	☐	☐	☒
Outline interview schedule / focus group schedule	☐	☐	☒
Debriefing materials	☐	☐	☒
Health and Safety Risk Assessment Form	☐	☐	☒

[3] It is mandatory to attach the Participant Information Sheet (PIS)
[4] It is mandatory to attach a Participant Consent Form, unless it is embedded in an online survey, in which case your supervisor must approve it before you start data collection

Appendix C: Information Sheet and Consent form

GUIDANCE ON PREPARING A PARTICIPANT INFORMATION SHEET

The following issues should be addressed where relevant. This could be, but does not have to be, in a question-answer format. Use a format that best meets the needs of your research participants, but the list below summarises the areas that need to be addressed to ensure participants are appropriately informed. Plain easily-understood language should be used with a minimum of technical or academic terms or jargon. Pay special attention to preparing material for children or adults with limited cognitive capacity - further information on this can be obtained from www.hra-decisiontools.org.uk/consent/

List of Contents Required: They do **not** have to be presented in this order as numbered questions; rather this list provides a checklist of the material that is now required to be in a Participant Information Sheet or equivalent briefing under GDPR.

1. **Title of Project:** Anomaly Detection to Provide Enhanced Security During Video Surveillance

2. **Legal basis for research for studies**:
   The University undertakes research as part of its function for the community under its legal status. Data protection allows us to use personal data for research with appropriate safeguards in place under the legal basis of **public tasks that are in the public interest.** A full statement of your rights can be found at: www.shu.ac.uk/about-this-website/privacy-policy/privacy-notices/privacy-notice-for-research. However, all University research is reviewed to ensure that participants are treated appropriately and their rights respected. This study was approved by the University's Research Ethics Committee with reference number *xxxxxxx*. Further information at: www.shu.ac.uk/research/excellence/ethics-and-integrity

3. **Opening statement:** You are invited to take part in a research study as part of a postgraduate dissertation in MSc Big Data Analytics at Sheffield Hallam

University. This project investigates how anomaly detection techniques can enhance the accuracy and reliability of security in video surveillance systems.

4. **Why have you asked me to take part?**
   You are being invited because you have basic knowledge of security, surveillance, or are a student/volunteer willing to give feedback on system outputs.

5. **Do I have to take part?**
   No. Participation is entirely voluntary. You can withdraw from the study at any point before submitting your response, and you do not have to give a reason.

6. **What will I be required to do?**
   You will be shown example output from an anomaly detection model and asked to provide feedback via a short questionnaire.

7. **Where will this take place?**
   This study will take place online. You will be invited to complete a short survey remotely using a secure online platform (such as Google Forms). You can take part at a time and location convenient to you using your own device.

8. **Are there any risks or benefits?**
   There are no risks. While there are no direct benefits, your input will help improve anomaly detection systems in real-world surveillance.

9. **Will my data be confidential?**
   Yes. Your responses will be kept anonymous and used only for academic purposes. No personal identifying information will be collected.

10. **What happens to the data after the study?**
    Data will be stored securely for the duration of the research and then deleted. It will not be shared outside the project.

11. **Who is responsible for this research?**

This study is conducted by a postgraduate student at Sheffield Hallam University. If you have any concerns, you may contact:

Student Researcher: Sandeep Babu Sampenga, sandeepbabu.b.sampenga@student.shu.ac.uk

Supervisor: Mansi Khurana, m.khurana@shu.ac.uk

Researcher/ Research Team Details:

You should contact the Data Protection Officer if:	**You should contact the Head of Research Ethics (Dr Mayur Ranchordas) if:**
• you have a query about how your data is used by the University • you would like to report a data security breach (e.g. if you think your personal data has been lost or disclosed inappropriately) • you would like to complain about how the University has used your personal data DPO@shu.ac.uk	• you have concerns with how the research was undertaken or how you were treated ethicssupport@shu.ac.uk
Postal address: Sheffield Hallam University, Howard Street, Sheffield S1 1WBT Telephone: 0114 225 5555	

Participant Consent Form

TITLE OF RESEARCH STUDY: Anomaly Detection to provide Enhanced Security during Video Surveillance

Please confirm the following before proceeding:

☒I have read and understood the Participant Information Sheet.

☒I understand that my participation is voluntary, and I can withdraw at any time before submission.

☒ I consent to take part in this study.

☒ I understand that the data I provide will be kept confidential and used only for academic purposes.

☒ I agree that anonymised data may be used in future research or publications.

Participant's Signature: Gnana Deepika Bodempudi Date: 1st September 2025

Participant's Name (Printed): Gnana Deepika Bodempudi

Contact details: +44 7447650746
Mail ID: bodempudideepika@gmail.com

Researcher's Name (Printed): Sandeep Babu Sampenga

Researcher's Signature: Sandeep Babu Sampenga

Researcher's contact details:
(Name, address, contact number of investigator)

Sandeep Babu Sampenga,

The forge, Sheffield,

S2 4QA,

+44 7436193973.

Please keep your copy of the consent form and the information sheet together.

Appendix D: Dataset and Codes

Link for Dataset:

UCSD_Anomaly_Dataset

Link for Code:

https://github.com/sandeepsampenga9700-dotcom/Anamoly-Detection-Survilliance