Secure System for Anomaly Detection and Data Analysis in The Arbaeen Pilgrimage Using ML Algorithms

Lect. Dr . Safa S. Abdul-Jabbar

University of Baghdad – College of Science for Women – Department of Computer Science

safa.s@csw.uobaghdad.edu.iq

Prof.Samira Naji Kadhim

University of Baghdad – College of Science for Women

samirank_math@csw.uobaghdad.edu.iq

Abstract

Religious events are held globally, where the Arbaeen pilgrimage is considers one of the largest events. During this event, millions of visitors arrive in Iraq from different countries, creating an urgent need to ensure a safe and organized mass movement for people and vehicles. Therefore, in this research an intelligent framework for crowd movement analysis and anomaly detection was designed specifically for this event. Synthetic datasets were created to simulate the dynamics of the visit and test the proposed framework. Six machine learning algorithms were applied (Isolation Forest, Local Outlier Factor (LOF), Rolling Z-Score, ARIMA Residuals, DBSCAN Clustering, and Kernel Density Estimation (KDE)) to analyze Data identify anomalies (such as sudden overcrowding or irregular movement patterns) which may indicate possible threats to safety, unusual stops, or irrational movements. In addition to calculating the accuracy of each algorithm by comparing its results with the majority vote results and measuring the execution time of each algorithm. Moreover, to maintain data privacy and integrity, with the results signed using a digital signature (SHA3-256) to ensure security and integrity. The system aims to support the shrine authorities by monitoring crowd behavior and enabling proactive measures to enhance the safety of visitors and the smooth execution of procedures.

Keywords: Anomaly Detection, Human Crowds, Vehicle Movements, Arbaeen Pilgrimage, Surveillance System.

Introduction

Arbaeen Pilgrimage is annually religious procession in Iraq that attracts approximately twenty million participants (Al-Ansari, F., Al Ansari, M., Hill-Cawthorne, G. A., Abdulzahra, M. S., Al-Ansari, M. B., Al-Ansari, B., ... & Conigrave, 2020). one of the most complex issues is how to manage crowd data. these issues require a multilayered framework with incorporates various strategies and methods to ensure an efficient crowd management (Siddiqa, A., Khan, W. Z., Alkinani, M. H., Aldhahri, E. A., & Khan, 2024) (Bhardwaj, S., & Singh, 2022). Consequently, any crowded data must analyze to indicates irregular or uneven patterns commonly referred to as anomaly. Anomaly refers to any unusual or different event (i.e. abnormal event or behavior). The classification of an individual's behavior as abnormal depends on the nature of the event, the type of activity in the surrounding environment and whether the individual is alone or part of a group. The identification of abnormal behavior also varies including the nature of the activity, its location, its context, location, number of participants, and other situational factors (Aldayri, A., & Albattah, 2024). Traditional crowd management systems are not only time- and resource- consuming, are also considered inadequate for managing the complexity of large data generated from massive crowds and effect the safety and security of peoples. Therefore, artificial intelligent models have been employed as an effective solution to automate crowd analysis and anomaly detection (Bhuiyan, M. R., Abdullah, J., Hashim, N., Al Farid, F., Haque, M. A., Uddin, J., ... & Abdullah, 2022). Therefore, to maintain the security and integrity of the crowd while reducing the disturbances and ensuring the safe movement of people and vehicles. There are two primary obstacles in designing any crowd management system: real-time processing of big data and privacy-preservation issues (Siddiqa, A., Khan, W. Z., Alkinani, M. H., Aldhahri, E. A., & Khan, 2024) (Bhardwaj, S., & Singh, 2022). The main contributions of this paper are:

- Analyzing vehicles and people movement data during the Arbaeen Pilgrimage, using multiple methods of machine learning (Isolation Forest, Local Outlier Factor (LOF), Rolling Z-Score, ARIMA Residuals, DBSCAN Clustering, and Kernel Density Estimation (KDE)) to detect anomalies such as abnormal speeds, unusual stops, or irrational movements, determining the accuracy of each algorithm.
- Approving the final results through the voting method in the best ways used.
- Signing the results using a digital signature (SHA3-256) to ensure security and integrity.

This paper consists of several main sections including: Section 2 presents the related work, including a review of recent papers on anomaly detection. Section 3 introduces the main tools and techniques used for analyzing the input data and detecting anomalies. The results are presented in Section 4, while the main conclusions and suggestions for future work are discussed in Section 5.

Related works

Crowed data analysis and anomaly detection have become critical concerns and important subject to improve the safety aspect for people in different events whether it is religious or other occasions (Mudgal, M., Punj, D., & Pillai, 2021). Crowed management systems are an essential tool for managing the movement of people and vehicles to provide a safe and secure environment for them. In recent years, the growing demand for digital and online systems has pushed event organizers and management system researchers to a new level(Haghani, M., Coughlan, M., Crabb, B., Dierickx, A., Feliciani, C., van Gelder, R., ... & Wilson, 2023).

A hybrid anomaly detection framework for identifying fraudulent electricity consumption using supervised and unsupervised machine learning algorithms was introduced by Oprea et al. In 2021 which provide a maximum detection accuracy equal to 90% by addressing the challenge of detecting consumption anomalies in large unnamed smart meter datasets, where traditional methods struggle with accuracy and scalability by proposing a two-stage approach, the first stage was to use residual spectral convolutional neural networks and Martingale-based models to detect anomalies, and then classify the result using two-class augmented decision trees and linear discriminant Fisher Analysis to validate and optimize suspicious markers system (Oprea, S. V., Bâra, A., Puican, F. C., & Radu, 2021). In 2022, Tiwari presented a research study that focused on the challenges associated with detecting missing values, outliers, and inconsistencies that occur when integrating data from multiple sources across different domains, including finance, healthcare, and cybersecurity. The proposed framework used a hybrid system combining traditional statistical methods with classical machine learning models such as random forests and support vector machines, along with deep learning techniques such as autoencoders and LSTM networks, to process structural and temporal data. A set of advanced analytical tools were used within the system in order to obtain high efficiency when dealing with big data. These tools contribute to enhancing the system's ability to detect abnormal patterns with greater accuracy (Tewari, 2022).

Similarly, in 2023, Jadhav et. al. produced an intelligent monitoring system that works to instantly detect abnormal behaviors in crowds and relies mainly on deep learning techniques, as it integrates full convolutional neural networks (FCN) with LSTM networks, to process and analyze video directly. A high accuracy rate has been achieved. It reached 97.84% to detect anomalies without errors such as false alarms or exceeding real alarms. This enhances the reliability of the proposed system in crowded environments that require quick decisions and accurate response (Jadhav, C., Ramteke, R., & Somkunwar, 2023).

In an effort to go beyond the limitations inherent to traditional models that rely solely on superficial visual features, in 2024 Fania and his team introduced an innovative model based on emotional features in the analysis of crowd behavior, making use of stress and emotion indices for a deeper understanding of the nature of collective behaviors in dynamic and complex environments. The core idea was to use collective emotions – such as anger, joy, and fear – as a medium to represent behavior. A huge database of 35 video sequences and more than 40,000 clips encoded with behavioral and emotional tags has been collected. With using algorithms such as SVM, the model has shown an improvement in the accuracy of detecting abnormal behaviors by more than 7% compared to traditional methods, with a notable advantage in recognizing situations such as "panic," despite some challenges in behaviors such as "crowding" in which movements overlap (Vaniya, J. H. K., Gamit, N. C., Trivedi, N. S. B., Chand, C. G., & Varia, 2024). In 2024, Park et al. also presented a practical solution to enhance security in residential and office environments through an intelligent monitoring system based on facial recognition technology using the HOG algorithm. The system is distinguished by its ability to instantly recognize faces stored in the database and trigger an alert when unfamiliar people approach. What distinguishes this system is not only its integration with live surveillance cameras, but also its support for interacting with smartphones, allowing the user to control remotely by viewing video, sending an alarm, or quickly reporting to the competent authorities. Together, these advantages make this system an effective and low-cost option compared to traditional security systems (Park, J. K., Yoon, J. W., & Kim, 2024). Also, in 2024, Shah published a study proposing a model for classifying crowd density during Hajj into three main categories: moderate, severe, and very dense. The model was based on feature extraction using the LBP method, taking into account the density of edges and the space occupied in each frame. The model was tested on 18 videos of different pilgrimage sites, achieving an assessment accuracy of 87% and a low error rate of 2.14%. This model contributes directly to support safety management decisions during seasons with heavy human flow (Shah, 2024). To simplify, the published papers discussed in this section are summarized in the following table.

Table 1: Related Works Summary

Ref.	Main Findings	Performance metrics	Limitation	Main Contribution	Main Techniques
(Oprea, S. V., Bâra, A., Puican, F. C., & Radu, 2021)	Combining unsupervised and supervised machine learning methods significantly improves fraud detection.The effective threshold-based labeling of anomalies is (>15%)	Accuracy:90%, Precision:0.875, F1-score: 0.894	Applied on only recorded data, not on real-time data	Hybrid ML framework that bridges the gap between unlabeled time-series data and fraud prediction Introduced a two-stage detection pipeline.	SR-CNN, Boosted, Decision Tree, and Fisher Linear Discriminant Analysis. Chi-squared statistics and Fisher Score for feature selection
(Tewari, 2022)	Traditional models like SVM showed lower performance. LSTM ans Autoencoders outperformed the others methods.	LSTM achieved 96.4%, Autoencoders 95.1%;	Eliminate the missing and duplicated values and correct the inconsistency of data	Design and evaluation of a hybrid anomaly detection system using machine learning and deep learning	Long Short-Term Memory (LSTM), Autoencoders Support Vector Machine (SVM)
(Jadhav, C., Ramteke, R., & Somkunwar, 2023)	Developed a deep learning system combining FCN and LSTM for real-time monitoring of crowds and suspicious activity detection.	Accuracy: 97.84%; significant reduction in false positives/negatives	Limited evaluation on diverse conditions; may still be sensitive to occlusions or lighting changes	Created an intelligent surveillance framework for accurate suspicious behavior detection. Reduced manual intervention	Fully Convolutional Network (FCN), LSTM, Deep Neural Networks

Ref.	Main Findings	Performance metrics	Limitation	Main Contribution	Main Techniques
(Vaniya, J. H. K., Gamit, N. C., Trivedi, N. S. B., Chand, C. G., & Varia, 2024)	Using crowd emotions as mid-level features. Improves behavior recognition compared to relying only on low-level visual features	Accuracy: 71.87% (best for "panic" behavior), 43.64% with Dense Trajectory	Overlapping motion patterns. Lack of emotion labels at test time	Introduced a new annotated dataset (crowd behavior + emotion), and a novel emotion-based and latent emotion approach for behavior classification	SVM, Dense Trajectory, Emotion-based classification, Latent SVM
(Park, J. K., Yoon, J. W., & Kim, 2024)	Implemented a real-time surveillance system using HOG-based face recognition to detect and alert unauthorized entries in home and office environments.	system emphasizes the ability of real-time processing and low computational complexity.	Potential challenges in varying lighting conditions and occlusion. Limited scalability for large datasets.	Developed a cost-effective and efficient surveillance system. Integrate motion detection and face recognition using HOG.	Histogram of Oriented Gradients (HOG), Motion Detection Algorithms. Face Recognition Techniques.
(Shah, 2024)	Developed a model to classify Hajj crowd density into three levels with real-time alert via red light for critical density.	Accuracy: 87% Error Rate: 2.14%	Limited to pre-recorded video data. May not generalize to real-time. unseen crowd conditions or other environments.	Introduced a lightweight ML-based system combining texture, edge, and spatial features for crowd density detection.	Local Binary Pattern (LBP), edge density, space occupancy, supervised ML classifier

Materials and methods

This research developed an intelligent model capable of detecting anomalous patterns for people and vehicles movement data of within crowed environment. The proposed system , shown in Figure 1, focuses on the analysis of behavioral data generated specifically for the purpose of research, applying a selection of anomaly detection algorithms belonging to different styles of machine learning techniques, with the aim of comparing their performance and determining the most appropriate in terms of accuracy, time and ability to detect unusual behavior. The work includes a set of main stages that begin with collecting and processing data, then applying algorithms, analyzing and signing the results.

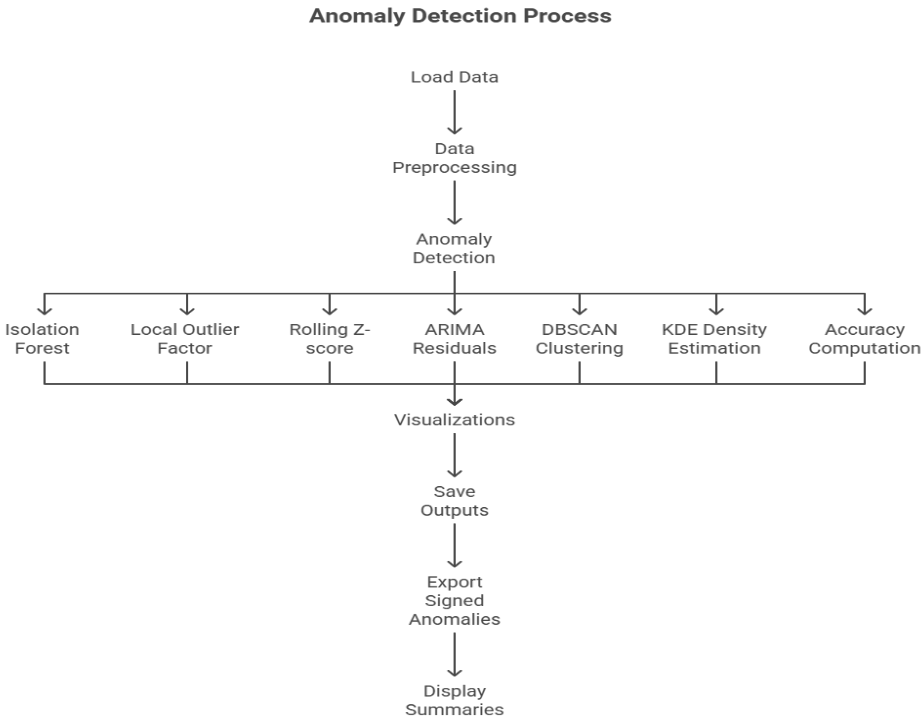


Figure 1: The general flowchart of the proposed system

Semi-Annual Scientific Journal www.arbnj.com Ramadan 1447 A.H, March 2026 A.D

1.Data collection:

Two sets of data were generated: the first simulates the movement of people, and the second represents the movement of vehicles in virtual environments that were designed to mimic real scenarios. Each group contained 3,000 records, with 3,000 entries generated for both the pedestrian and vehicle datasets using custom Python code. The values—numerical, temporal, and spatial—were randomly generated while preserving the internal logic and consistency of the data. An additional 3,000 fields were also produced using AI tools, which used artificial generation models to simulate more realistic behavior based on virtual reference data. These data were saved in Excel format for use in subsequent analytical processes.

2.Data Processing:

The data was subjected to a series of pre-processing operations, which included converting time fields into a type (Datetime), and extracting derived attributes such as the clock from the time of movement. Numerical fields such as stop duration, time difference, and average speed have been converted into scalar values that can be processed. Missing values were processed and incomplete records deleted. Standard scaler has also been used to standardize values when needed, especially.

before applying some algorithms such as Local Outlier Factor. All these operations contributed to Improving detection accuracy and reducing the possibility of error.

3.ML Algorithms Selection:

In this system, six main anomaly detection algorithms were selected, representing different trends in the field of machine learning:

- Isolation Forest: This algorithm belongs to unsupervised learning methods and is based on the idea of isolating anomalous records by building a number of random trees. They were chosen for their high ability to detect anomalies in high-dimensional data and their ease of application to large datasets (Liu, F. T., Ting, K. M., & Zhou, 2012).
- Local Outlier Factor (LOF): This algorithm is unsupervised anomaly detection algorithms and based on comparing the local density between the point in question and its neighbors, and determining the anomaly based on the deviation from the surrounding density. It is effective in detecting abnormal patterns surrounded by natural records, and represents a method of unsupervised learning (Breunig, M. M., Kriegel, H. P., Ng, R. T., & Sander, 2000).
- Rolling Z-Score: This technique is statistical, and relies on calculating the moving standard deviation to identify points that exceed the limits of the triple deviation, which may indicate an anomalous pattern. They were used due to their simplicity and ability to detect sudden time changes (Anusha, P. V., Anuradha, C., Murty, P. C., & Kiran, 2019). The standard equation for Z-score can described in eq (1).

$$z = \frac{x - \mu}{\sigma} \qquad (1)$$

Where, x is the current value, μ is the mean of the previous n values, and σ is the standard deviation of the previous n values.

- ARIMA Residuals: This method is particularly effective in scenarios where time is a key factor influencing behavior change. It relies on modeling the time series using the ARIMA model and then analyzing the residuals (i.e., the differences between predicted and actual values) to detect deviations from expected patterns. We can distinguish this approach by its predictive capability, which allows for the detection of time-based anomalies by leveraging the temporal structure of the data (Braei, M., & Wagner, 2020).
- DBSCAN Clustering: this method is spatial movement analysis (i.e. if we use the density to identify clusters, and detects anomalies then the DBScan can used which classify points that do not belong to any cluster as anomalous). This algorithm is useful in analyzing geographical locations to identify unusual locations of vehicle movement (Yue, X., Wang, C., Wang, Y., Chen, L., Wang, W., & Lei, n.d.).
- KDE (Kernel Density Estimation): Finally, the proposed system used the technique of estimating the density of the distribution of points in space to identify anomalous values based on the density drop surrounding those points. This method is particularly suitable for analyzing geographic and spatial data(Chen, 2017).

4.Group voting mechanism and accuracy analysis:

This approach aims to increase reliability and mitigate the potential impact of individual classification errors. After implementing all the ML algorithms for detecting anomalies, a decision-making mechanism was developed based on a consensus voting approach, such that a record is considered anomalous only if at least three algorithms classify it as abnormal. To evaluate performance, the accuracy of each algorithm is calculated by matching its results with the decisions of the voting system. The time for implementing each algorithm was also measured using time measurement tools built into the Python language, to measure the efficiency and accuracy of each technology used.

5.Digital signature and data protection:

In the context of enhancing the reliability of results and protecting the integrity of data classified as anomalies, a numerical integrity assurance mechanism has been adopted consisting in the creation of unique digital signatures for each record classified as out of pattern (Gilbert, C., & Gilbert, 2025). The secure hashing algorithm SHA3-256 was used for this purpose, relying on combining temporal information with motion change indicators, providing a digital fingerprint that is not repeatable or tamper-evident. These signed records are saved in a separate CSV file, which serves as a documented record of all anomalies detected by each algorithm, ensuring that they can be referred to in future evaluation and verification reports.

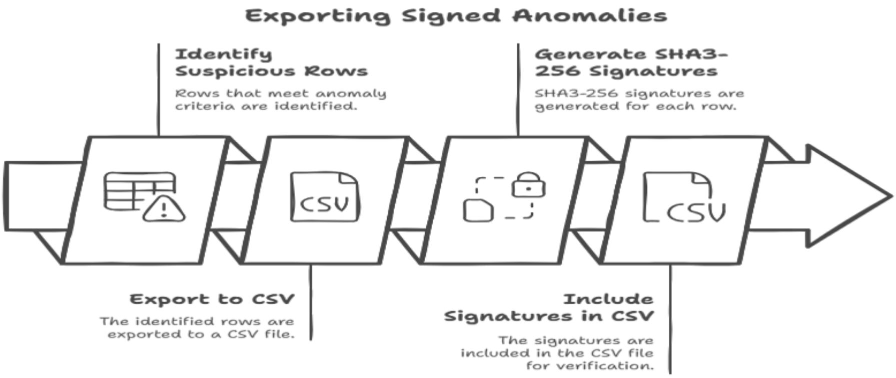


Figure 3: the main steps for Digital signature and data protection

6.Storing results and analyzing performance:

As a final step in the proposed system, all results obtained from the previous stages were stored in structured Excel files (e.g., classification details, execution times, accuracy ratios, and digital signatures associated with anomalous records). Additionally, all training, testing, and validation outcomes were visualized through interactive graphs, illustrating patterns of anomalies, correlations between algorithms, temporal performance variations, and classification outcomes based on the consensus voting mechanism. This approach enables users to gain a deeper understanding of data behavior and to evaluate the effectiveness of each algorithm across various testing environments.

Results and Discussion

The proposed system was evaluated using two types of data that were mentioned in Session 3.1 (pedestrian and vehicle) from several aspects, including time, performance, and security the results were as shown in the following sections.

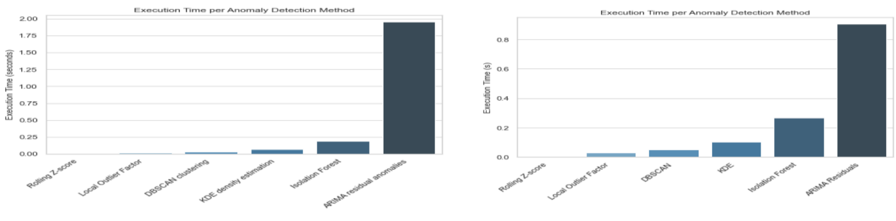
1.Execution time:

One of the most prominent challenges facing the design of intelligent anomaly detection systems is the necessity of combining accuracy of results with speed of response. The high performance of algorithms is not only measured by accuracy, but the execution time factor must be taken into account, especially in time-sensitive applications such as crowd monitoring or real-time vehicle tracking. To achieve a comprehensive assessment, two datasets representing two different types of movements were adopted one for pedestrian movement and another for vehicle behavior as illustrated in Table 1 and showed in Figure 3. The algorithms were tested on each group separately to accurately measure the execution time. In terms of vehicle data, the Rolling Z-score algorithm emerged as the fastest, with a time of about 0.002 seconds, followed by LOF and DBSCAN, while the Isolation Forest and ARIMA algorithms took relatively longer. This gradient in performance reflects a natural variation based on the complexity of each algorithm. In the case of pedestrian data analysis, the Rolling Z-score achieved exceptional performance with a time of only 0.001 seconds, making it very suitable in situations that require immediate detection, such as sudden gatherings or unexpected behaviors in public places. Then came the LOF algorithm with a reasonable time, followed by DBSCAN and KDE, while ARIMA recorded the longest execution time, at nearly two seconds, which is in line with its statistical nature based on a sequential analysis of temporal data.

The most notable aspect of these results is not only the differences in execution time, but also the clear consistency in the behavior of the algorithms when applied to two different types of data. This stability indicates the flexibility of the system and its ability to adapt, whether the data is related to the movement of individuals or vehicles. From an applied perspective, this temporal analysis does not only aim to classify algorithms according to their speed, but also opens the door to designing anomaly detection solutions that can be customized according to the nature of the task. Balancing time efficiency and detection accuracy represents the cornerstone of any system used in dynamic environments that require immediate decisions.

Table 1: The Execution time Classification

Algorithm	Execution Time (seconds) for Pedestrians	Execution Time (seconds) for Vehicle
Rolling Z-score	0.001142	0.002067
Local Outlier Factor	0.015395	0.029716
DBSCAN clustering	0.027582	0.048225
KDE density estimation	0.063402	0.100840
Isolation Forest (IF)	0.188649	0.267273
ARIMA residual anomalies	1.954967	0.902721

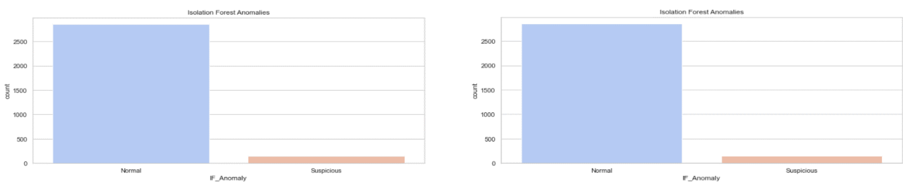


(a) (b)

Figure 3: The execution time for both: (a) Pedestrians dataset, and (b) Vehicle dataset

2.Performance evaluation:

To evaluate the system performance for the Pedestrians and Vehicle data we select six anomaly ML algorithms as mentioned in section (3.3). Figure 4 shows the results of applying the Isolation Forest algorithm to the Arbaeen Pilgrimage data preprocessing operations (Converting time fields into DateTime format, extracting derived attributes, converting numerical fields into processable values, in addition to processing missing values and standardizing values using Standard Scaler). The first image represents the movement of walking people, while the second image represents the movement of vehicles. The results in both figures show that most records were classified as “normal,” while a limited number of “suspected” or “abnormal” cases were detected. This pattern reflects the regularity of overall behavior within both human and vehicle data, with a few exceptions indicating unusual movement patterns.



(a) (b)

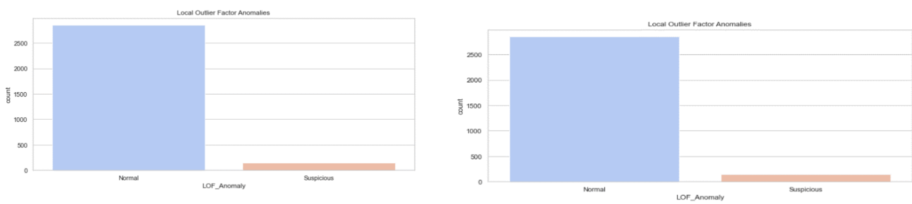
Figure 4: Applying Isolation Forest algorithm for both: (a) Pedestrians dataset, and (b) Vehicle dataset

We also notice in the results of Figure 5 that show the application of the Local Outlier Factor (LOF) algorithm to the data of Pedestrians (a) and vehicles (b) during the Arbaeen Pilgrimage, where a small percentage of abnormal values were detected compared to normal cases in both groups.

The LOF algorithm relies on measuring the local density of points, making it effective in identifying unusual behavior in areas with a heterogeneous data distribution. The results show that LOF was able to isolate a limited number of records as suspects, indicating that general patterns of movement — of both people and vehicles — are characterized by a high degree of frequency and similarity within the temporal and spatial context of the visit.

It can also be seen that the performance of LOF was consistent in the two cases,which is a confirmation of its ability to handle different types of data after the careful pre-processing carried out. This consistency may be the result of the effectiveness of normalization and standardization of numerical values, which limits the influence of heterogeneous distributions that may affect the accuracy of detection.

From another perspective, these results highlight that density-based algorithms such as LOF are able to detect cases that may not be considered anomalies based only on statistical values, but also according to the neighborhood relationships and local environment of each point, which gives an additional dimension to analyzing behavior during major events.



(a) (b)

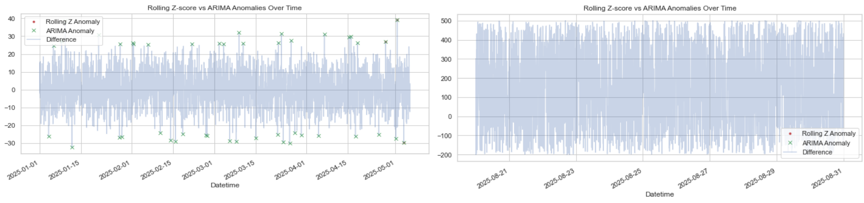
Figure 5: Applying Local Outlier Factor for both: (a) Pedestrian dataset, and (b) Vehicle dataset

Though Figure 6, a visual comparison was made between the Rolling Z-score and ARIMA algorithms to detect anomalies within people and vehicle data during the Arbaeen Pilgrimage, by tracking the differences over time.

In image (a) we observe an overlay between the results of the two algorithms, with only some cases detected by ARIMA (shown with green Xs), while the Rolling Z-score algorithm (red dots) showed higher sensitivity in some temporal locations. The shaded area (the difference between values) also helps highlight how close or far apart the detection results are over time, indicating a slight difference in each algorithm's interpretation of the normal versus abnormal pattern.

While in image (b) we observe a relatively lower variability between the results of the two algorithms than in the first image, reflecting a greater stability in the vehicles data. The ARIMA algorithm shows some anomalies that were not captured by Rolling Z-score, which may indicate its ability to analyze precise trends in time, especially in data that follows regular sequential behavior.

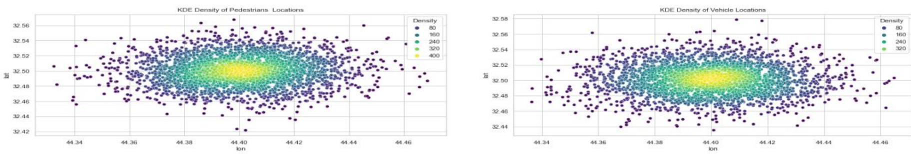
In short, these results reflect that the performance of the two algorithms varies depending on the nature of the data used. Rolling Z-score shows speed and immediate response to sudden situations, while ARIMA excels at analyzing repetitive and complex time patterns. This contrast supports the idea of combining more than one algorithm to achieve balanced detection that combines speed and accuracy, especially in live environments that require thoughtful, instantaneous decisions.



(a) (b)

Figure 6: Comparison between Rolling Z-score and ARIMA for both datasets: Pedestrian data, and (b) Vehicle data.

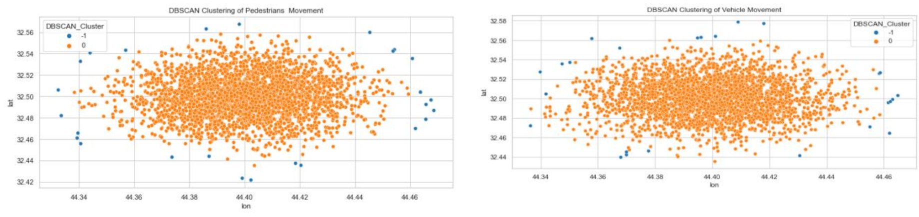
On the other hand, the results of Figure 7 show the spatial density of pedestrian and vehicular traffic using KDE (Kernel Density Estimation) technology. Zones (a) and (b) show a clear concentration in a specific geographical area, showing the presence of a central attraction during the Arbaeen Pilgrimage. Also, brighter colors (yellow and green) indicate the highest accumulation of movement, which can support field organization and management plans. Comparing the two drawings shows the similarity of spatial distribution, with a slightly higher density of pedestrian movement.



(a) (b)

Figure 7: The KDE Density for both datasets: Pedestrian data, and (b) Vehicle data.

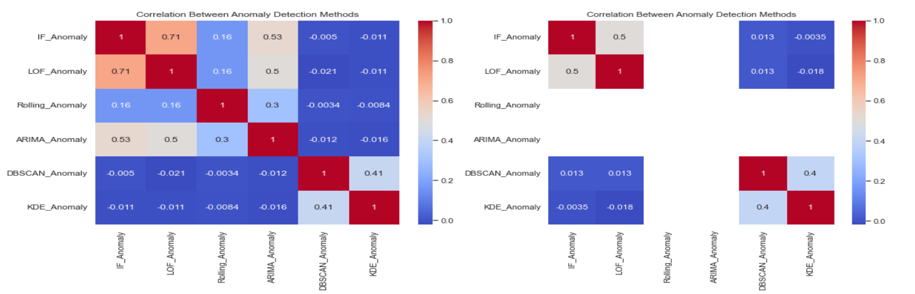
The results in Figure 8 show a probability density analysis (KDE) of pedestrian (a) and vehicle (b) movements using the DBSCAN algorithm for clustering. It is clear from the figure that the basic intensity of movement is concentrated in the center of the geographical area, with some scattered points (noise) on the periphery. This indicates that most activity, whether pedestrian or vehicle, takes place within a specific range, while movements outside this range are uncommon. The distribution of points also shows relative similarity in the general shape of both types of data, which may indicate partial overlap in movement patterns within the studied environment.



(a) (b)

Figure 8: The DBSCAN Density for both datasets: Pedestrian data, and (b) Vehicle data.

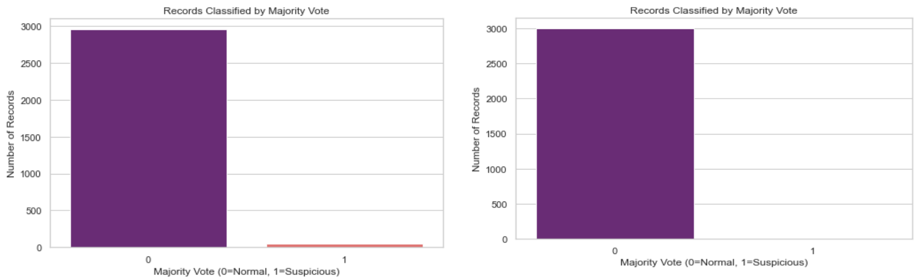
On the other hand, the correlation matrix in Figure 9 illustrates the correspondence between the anomaly detection methods in pedestrian data (a) and vehicle data (b). In the pedestrian data, a strong correlation is observed between the IF and LOF methods (0.71), as well as between ARIMA and IF (0.53), indicating a similarity in the results of these methods. In the vehicle data, however, most of the values are weak, showing a large variation in the performance of the different methods. This indicates that the nature of the data affects the compatibility of anomaly detection tools, and it is preferable to use more than one method to verify the results.



(a) (b)

Figure 9: The Correlation matrix for both datasets: Pedestrian data, and (b) Vehicle data.

Finally, Figure 10 shows the results of data classification using majority voting to detect suspicious cases, where the image represents (a) pedestrian data and (b) vehicle data. It is noted that the vast majority of records in both groups were classified as normal (0), with very few records classified as suspicious (1), indicating a scarcity of abnormal behavior in both cases.



(a) (b)

Figure 10: The classification results for both datasets: Pedestrian data, and (b) Vehicle data.

As a result of applying the system to this data and according to a vote for these algorithms, the results show that the ARIMA and Rolling algorithms excelled in detecting anomalies within pedestrian data, while LOF and KDE recorded the highest accuracy with vehicle data. This indicates that the effectiveness of detection algorithms depends greatly on the nature of the data used, as shown in Table 2.

Table 2: Accuracy Compared to Majority Vote for Pedestrians and Vehicles

Algorithm	Accuracy for Pedestrians	Accuracy for vehicles
ARIMA_Anomaly	0.997999	0.950984
Rolling_Anomaly	0.986329	0.950984
DBSCAN_Anomaly	0.976992	0.951651
IF_Anomaly	0.964988	0.991997
LOF_Anomaly	0.964321	0.998333
KDE_Anomaly	0.937646	0.998333

3.Security measurements:

The adoption of digital signatures represents a crucial step toward ensuring data integrity and enables the system to verify the tamper-proof nature of records classified as anomalies. As shown in Table 3, which serves as a visual representation of the security and reliability measures applied within the proposed anomaly detection system, the table lists the number of records identified as suspicious by each algorithm, along with the corresponding digital signature generated using the SHA3-256 secure hashing algorithm. This signature functions as a unique digital fingerprint that cannot be duplicated or forged, as it is derived from sensitive features of each record—such as timestamp and motion variation—thus enhancing both the credibility and integrity of the results.

Moreover, storing these signed records in a separate file (signed_anomalies_report.csv) provides a dependable reference for future use, whether for auditing, post-analysis validation, or scientific documentation. The variation in the number of detected anomalies across algorithms underscores the value of employing multiple detection techniques to reduce individual algorithmic bias and improve overall detection reliability. This approach is further reinforced in later stages of the system through the implementation of a consensus-based voting mechanism

Table 3: Anomaly Detection Summary for Pedestrians

Algorithm	Suspicious Count	SHA3-256 Signature
IF	150	7f3d8580bf6e24ba46c3e0d8ecbf392f68f64257fde6c198bd-f63624765ae46d
LOF	150	99870788603a748cd9bc0266f08de59d0ce38a6a6f7fb34d-0115434ed56fe8bd
KDE	150	30c8164d95c48fbb6df447b6edc5212f7f31b50382dad-b0e2ee2429ba7e14324
ARIMA	45	471ba78c641beb8f7ab3bf783bfcd6f7fb2faafb-5c2349530e43b4137317417f
DBSCAN	26	b03ce4e85b669b3cbe10ad661637f12357fa8bd1139b1d-314083c6cb17b414cf
Rolling	4	a5d19e51a3735fd42fe0b3f7dd55a60d32d88a3afad9a57bb-a5c82976a85017e

Table 4: Anomaly Detection Summary for Vehicles

Algorithm	Suspicious Count	SHA3-256 Signature
IF	150	c2b8d36b2489e23178127fcaf8953c441ff0742e5ef0dc7f-65688baf01a27a25
LOF	150	4eb6d6eed7326ae4d7fe06e29fc1d8224d-b32495101e328e1f98a5bdb61cabd6
KDE	150	b6b969e6bdf8db04ff4b10ca3f20bfb2e98951e6c-5827494de19bcd727ba9307
DBSCAN	25	b6b969e6bdf8db04ff4b10ca3f20bfb2e98951e6c-5827494de19bcd727ba9307
Rolling	0	b6b969e6bdf8db04ff4b10ca3f20bfb2e98951e6c-5827494de19bcd727ba9307
ARIMA	0	b6b969e6bdf8db04ff4b10ca3f20bfb2e98951e6c-5827494de19bcd727ba9307

Conclusions and Future Works

In this research, data related to the movement of vehicles and pedestrians during the Arbaeen pilgrimage were analyzed using a suite of anomaly detection algorithms following comprehensive preprocessing. These preparatory steps included converting time-related fields into analyzable formats, extracting derived attributes such as movement hours, and transforming numerical values—such as stop duration and average speed—into scaled forms suitable for algorithmic processing. Missing values were addressed, incomplete records were removed, and a standard scaler was applied to enhance the performance of certain algorithms, notably the Local Outlier Factor (LOF). The results demonstrated that unsupervised algorithms, such as Isolation Forest and LOF, were highly effective in detecting abnormal movement patterns in vehicle data without requiring pre-labeled training sets. Temporal analysis, utilizing models such as ARIMA and Rolling Z-Score, facilitated the identification of anomalies within specific time intervals, indicating potential irregularities in operational performance or traffic flow. Spatial analysis through DBSCAN and KDE enabled the detection of atypical geographic concentrations, which is essential for understanding crowd behavior during high-traffic periods.

The integration of temporal, spatial, and behavioral analyses enabled a more comprehensive understanding of anomalous movement dynamics, improving detection accuracy and bolstering the reliability of the system. This hybrid approach—merging conventional machine learning techniques with advanced statistical models and security tools—presents a robust and promising strategy for developing secure intelligent monitoring systems tailored to complex and safe operational contexts.

Despite the demonstrated effectiveness of the proposed framework, several avenues for future enhancement remain. Incorporating additional contextual variables—such as weather conditions, road quality, and traffic density—could refine model precision and support the detection of more complex anomalies. Moreover, the development of self-adaptive models using reinforcement learning may enable dynamic parameter tuning in response to changing environmental conditions. Implementing a real-time anomaly detection system would also facilitate immediate alerting, enhancing the responsiveness of operational and security teams. Finally, broader validation across diverse environments and incorporating human-in-the-loop verification could strengthen system credibility and enable more interactive and trustworthy decision-making.

Reference

1. Al-Ansari, F., Al Ansari, M., Hill-Cawthorne, G. A., Abdulzahra, M. S., Al-Ansari, M. B., Al-Ansari, B., ... & Conigrave, K. M. (2020). No Arbaeen public health concerns: a pilot cross-sectional survey. Travel Medicine and Infectious Disease, 35(101546).
2. Aldayri, A., & Albattah, W. (2024). A deep learning approach for anomaly detection in large-scale Hajj crowds. The Visual Computer, 40(8), 5589–5603.
3. Anusha, P. V., Anuradha, C., Murty, P. C., & Kiran, C. S. (2019). Detecting outliers in high dimensional data sets using Z-score methodology. International Journal of Innovative Technology and Exploring Engineering, 9(1), 48–53.
4. Bhardwaj, S., & Singh, V. (2022). Analysis of crowd behavior based on machine learning. International Journal of Modern Engineering Research (IJMER), 11(9(2)), 24–30.
5. Bhuiyan, M. R., Abdullah, J., Hashim, N., Al Farid, F., Haque, M. A.,

Uddin, J., ... & Abdullah, N. (2022). A deep crowd density classification model for Hajj pilgrimage using fully convolutional neural network. PeerJ Computer Science, 8(e895).

6. Braei, M., & Wagner, S. (2020). Anomaly detection in univariate time-series: A survey on the state-of-the-art. ArXiv Preprint ArXiv:2004.00433.
7. Breunig, M. M., Kriegel, H. P., Ng, R. T., & Sander, J. (2000). LOF: identifying density-based local outliers. In Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data, 93–104.
8. Chen, Y. C. (2017). A tutorial on kernel density estimation and recent advances. 1(1), 161–187.
9. Gilbert, C., & Gilbert, M. (2025). Exploring Secure Hashing Algorithms for Data Integrity Verification. SSRN 52516.
10. Haghani, M., Coughlan, M., Crabb, B., Dierickx, A., Feliciani, C., van Gelder, R., ... & Wilson, A. (2023). A roadmap for the future of crowd safety research and practice: Introducing the Swiss Cheese Model of Crowd Safety and the imperative of a Vision Zero target. Safety Science, 168(106292).
11. Jadhav, C., Ramteke, R., & Somkunwar, R. K. (2023). Smart crowd monitoring and suspicious behavior detection using deep learning. Revue d'Intelligence Artificielle, 37(4), 955.
12. Liu, F. T., Ting, K. M., & Zhou, Z. H. (2012). Isolation-based anomaly detection. . . ACM Transactions on Knowledge Discovery from Data (TKDD), 6(1), 1–39.
13. Mudgal, M., Punj, D., & Pillai, A. (2021). Suspicious action detection in intelligent surveillance system using action attribute modelling. Journal of Web Engineering, 20(1), 129–146.

14. Oprea, S. V., Bâra, A., Puican, F. C., & Radu, I. C. (2021). Anomaly detection with machine learning algorithms and big data in electricity consumption. Sustainability, 13(19), 10963.

15. Park, J. K., Yoon, J. W., & Kim, J. W. (2024). Implementation of surveillance system through face recognition using HOG algorithm. Library of Progress-Library Science, Information Technology & Computer, 44(2).

16. Shah, A. A. (2024). A machine learning model for crowd density classification in Hajj video frames. International Journal of Advanced Computer Science and Applications (IJACSA), 15(12). https://doi.org/https://doi.org/10.14569/IJACSA.2024.0151231.

17. Siddiqa, A., Khan, W. Z., Alkinani, M. H., Aldhahri, E. A., & Khan, M. K. (2024). Edge-assisted federated learning framework for smart crowd management. Internet of Things, 27(101253).

18. Tewari, S. (2022). Anomaly Detection in Large Scale Data Platforms with Machine Learning.

19. Vaniya, J. H. K., Gamit, N. C., Trivedi, N. S. B., Chand, C. G., & Varia, D. (2024). Analyzing and predicting crowd behavior using machine learning. International Journal of Intelligent Systems and Applications in Engineering (IJISAE), 12(4), 2027–2036. https://doi.org/https://doi.org/10.5281/zenodo.10926586.

20. Yue, X., Wang, C., Wang, Y., Chen, L., Wang, W., & Lei, Y. (n.d.). Gas flow meter anomaly data detection based on fused LOF-DBSCAN algorithm. In Proceedings of the 2022 11th International Conference on Computing and Pattern Recognition, 503–508.